Helsedirektoratet

PKI – strategi, status, utfordringer

Helsedirektoratet

Hvem er jeg?

- Godt spørsmål. Noen flere?
- Navn: Eirik Mangseth
- Stilling: Seniorrådgiver i Helsedirektoratet, avdeling for IT-strategi
- Jobbet med programvareutvikling/design/arkitektur siden 1991 frem til april i år.

Helsedirektoratet

PKI - strategi

- Strategien er lagt i Referansekatalog for IT-standarder i offentlig sektor, Versjon 2.0 (25.6.2009)
  - Kapittel 3.5 Standard for bruk av PKI med og i offentlig sektor
  - Kapittel 3.8 Standard for sikker elektronisk kommunikasjon
    - 3.8.2 spesielt rettet mot helsesektoren
      - Stiller krav til bruk av ebXML med PKI som sikkerhetsmekanismer
      - Konsekvenser:. Alle meldinger krypteres og signeres med virksomhetssertifikat. Enkelte meldinger signeres med personlig sertifikat.

PKI - historie

- Oppfunnet i England i 1969 av James Ellis som et svar på et forventet logistisk mareritt ved distribusjon av symmetriske kryptografiske nøkler til alle militære enheter og alt militært personell ifm ny plattform for sikker kommunikasjon.
- I 1973 fant den nyutdannede Clifford Cocks en matematisk funksjon som passet teorien til Ellis som hånd i hanske.

  ’From start to finish, it took me no more than half an hour. I was quite pleased with myself. I thought, "Ooh, that's nice. I've been given a problem, and I've solved it.”’
- Dessverre var ikke datidens datamaskiner kraftige nok til å ”make the possible practical” og i tillegg var alt arbeid vedr. kryptografi hemmeligstemplet, noe som hindret oppfinnerne fra å publisere oppdagelsen.
- Dermed lå feltet åpent for Diffie, Helman og Merkle som publiserte sine funn i 1977.

  Resten er historie som det så smukt heter.

Helsedirektoratet

PKI - historie

- PKI i helsesektoren
  - Forprosjekt for PKI i helsenett (2002).
    - Vurdering av helsesektorens PKI-behov, bl.a. knyttet til epikriser/henvisninger, resepter, sentrale helseregistre, NAV, m.m.
    - Anbefalte sikkerhetsnivå og sertifikatbehov
  - I 2004
    - krav fra Rikstrygdeverket om personlig digital signatur ifm. innsending av elektronisk sykmelding.
    - Rapport: Implementering av PKI i norsk helsevesen. Forslag til utrullingsplan for helseforetakene.
    - KITH-rapport 13/04: Anbefalinger og standarder for PKI i helsesektoren
  - KITH-rapport 12/05: Veiledning for innføring av ebXML og PKI i helseforetak
  - KITH-rapport 06/06: Prosjektrapport – Forprosjekt for PKI i helseforetakene
  - 2006: eResept, arkitektur: PKI i eResept
  - 2008: Programdirektiv, Nasjonalt meldingsløft 2008 – 2010
  - I tillegg var allmennpraktiserende leger (fastleger) tidlig ute med anskaffelse av digitale sertifikater, smartkortlesere, m.m.
  - Rammeavtale inngått av Ahus for PKI i spesialisthelsetjenesten

PKI – definisjon av

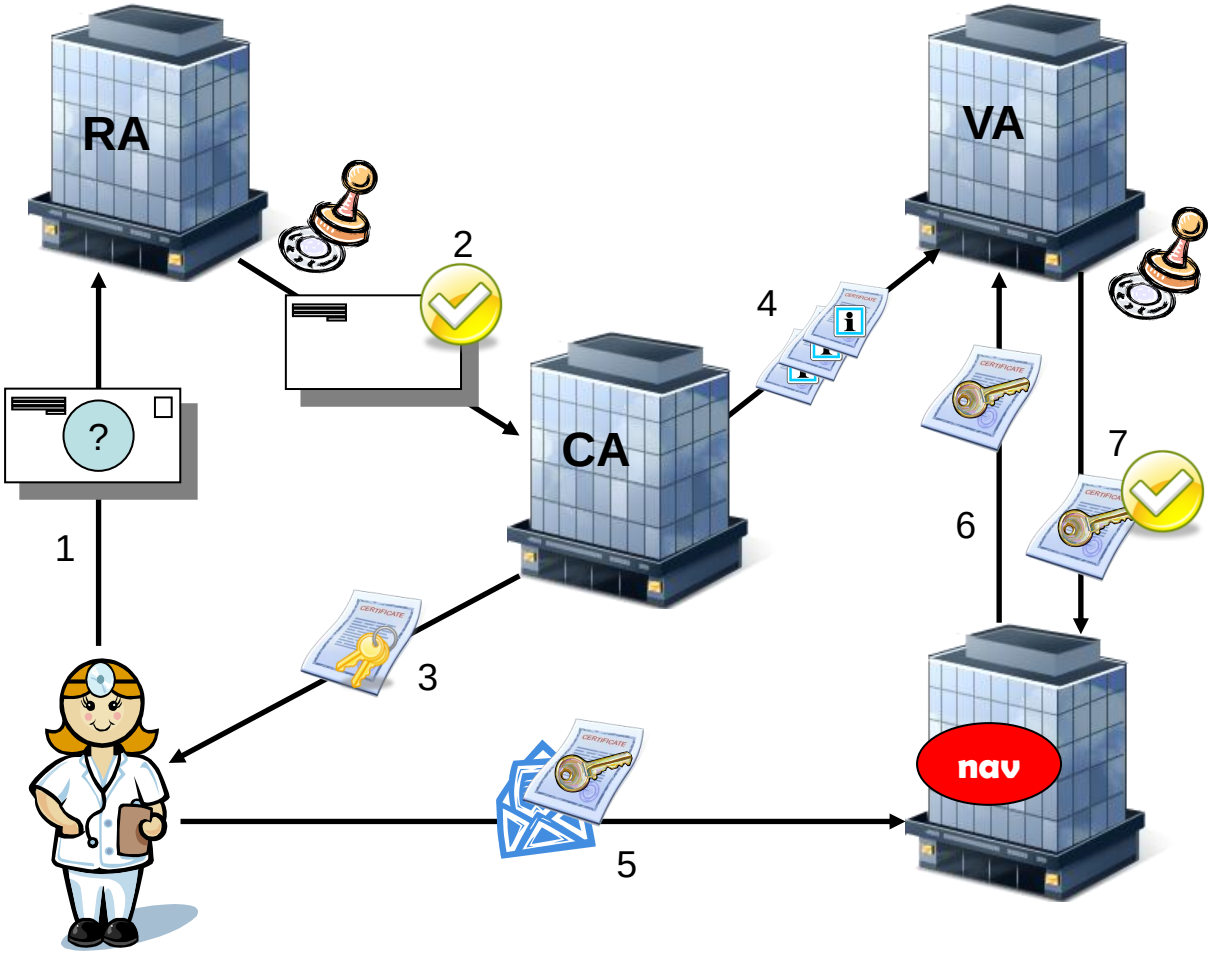
- **Public Key Infrastructure** (**PKI**) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates (kilde: wikipedia)
  - For helsesektoren håndteres dette p.t. av Buypass

PKI – digitale sertifikater

- *Digitale sertifikater* er det som benyttes til sikker meldingsutveksling mellom parter i Helsesektoren.
  - Brukes synonymt med PKI i sektoren.
  - Virksomhetssertifikater
    - benyttes primært til å sikre elektroniske meldingers *konfidensialitet, autentisitet og integritet*
    - *Ansvarliggjør helseforetak, legekontor*
  - Personlige sertifikater
    - Autentisering/identifisering av innehaver.
    - Signering av elektroniske meldinger (se integritet og autentisitet ovenfor).
    - Sikre uavviselighet
    - Ansvarliggjør den enkelte lege

Helsedirektoratet

PKI - Eksempelsenarie



PKI – implementering og bruk

- **Mål**
  - All informasjon mellom kommunikasjonsparter benytter PKI.
    - Personlig signatur benyttes på dokumenter som sykemelding, legeoppgjør og elektroniske resepter
    - Alle forsendelser signeres og krypteres med virksomhetssertifikater.
- Status
  - Fortsatt bruk av gamle standarder (DES-nøkler). Skal fases ut.
  - PKI tatt i bruk i deler av sektoren
    - Primærhelse: ca 1050 virksomhetssertifikater og ca. 3400 aktive personlige sertifikater
    - Helseforetak: virksomhetssertifikater brukes til MFR og POLK, personlige sertifikater til pålogging hos Ahus og St. Olavs
- Handlinger
  - Utbredelse av PKI til legekontor:
    - ved regionale meldingsløft
    - Ifm. utfasing av trygd-helsepostkassen
    - Legekontor/EPJ-leverandørene
  - Utbredelse av PKI til helseforetak
    - Kan eksisterende virksomhetssertifikat benyttes?
    - Hva med personlige sertifikater?

Helsedirektoratet

PKI – Utfordringer

- Logistikk og organisering
- Kostnader
- Bruk og sikkerhet

Helsedirektoratet

PKI - utfordringsbildet

- Er det god nok forståelse for hva digitale sertifikater/PKI er og hva det brukes til?
- Er det god nok informasjon hos ulike aktører?
- Er det god nok forståelse for ansvar og prosesser for anskaffelse og innføring av digitale sertifikater/PKI hos hhv legekontor og HF?
- Eller er det behov for å utarbeide en prosessbeskrivelse/anbefalt ansvarsfordeling i forbindelse med anskaffelsesprosessen?

Helsedirektoratet

PKI - Logistikk

- ”Amateurs talk about tactics. Professionals talk about logistics” (Gen. Schwarzkopf)
- Er vi kommet dit hen at det er logistikken som er den største utfordringen?
  - Tilbakemeldinger fra sektoren kan tyde på det.
  - Sektoren ønsker løsninger på nasjonalt nivå for
    - Bestilling, fornying, tilbakekalling, melding av tapt kort, m.m.
    - Valideringstjenester (Validation Authority), både for personlige sertifikater og virksomhetssertifikater
    - Integrasjon mot personalportaler, og lignende.
    - Der portalløsninger ikke finnes, kan man for eksempel benytte ID-porten eller liknende?
    - Profesjonskort med personlig digitale sertifikater? Vil kunne løse en del av anskaffelses- og fornyingsproblematikken.
    - Turnuskandidater
    - Utenlandske vikarer.

PKI - kostnader

- Anskaffelse, installasjon og fornyelse
- Legekontor
  - Virksomhetssertifikat
  - Smartkort og leser med tilhørende programvare
  - Muliggjør effektiv og sikker meldingsutveksling, så som legeoppgjør, sykmelding, legeerklæring, epikrise, eResept, m.m.
- HF
  - Virksomhetssertifikater
  - Smartkort pr. lege, lesere med programvare på nesten alle tilgjengelige PCer.
    - Profesjonskort vil kunne løse noen av utfordringene med korthåndtering
  - Eventuell integrasjon med personalportal, eller lignende.

PKI – bruk og sikkerhet

- Et smartkort inneholdende et eller flere digitale sertifikater er å betrakte som et verdipapir på lik linje med for eksempel et pass.
- Smartkortet med tilhørende PIN-kode er personlig og må ikke deles med andre.
- EPJ-systemene bør ikke mellomlagre PIN-koden over lengre tid
- Utfordringer med felles meldingstjener
- Sikker autentisering gir mulighet for bedre kontroll ved tilgang til helseopplysninger.
  - Tilgang på tvers, føderert identitet

PKI – Nasjonale løp

- Helsesektoren i det nasjonale eID-løpet
  - Direktoratet har god dialog med Difi og andre aktører utenfor sektoren
  - Viktig at sektorens behov for rett sikkerhetsnivå (nivå 4) blir ivaretatt
  - En god eID kan benyttes i hele EU-sonen
    - Ref. EU-prosjekt STORK.

PKI – lys i tunnelen(?)

- ”… det er nå derfor ingen vei utenom å installere PKI snarest mulig for dem som ikke allerede har dette på plass”
- Ad HELFO: ”De som har erfaring med løsningen er svært fornøyd og opplever den som ”et lys i det digitale helsemørket”… Kople dere opp!”
  - Jan Emil Kristoffersen i brev til medlemmene av Allmennlegeforeningen