Asymmetrisk krypto i pass og ID-kort = PKI + éngangsnøkler

Dr. Tage Stabell-Kulø

Unibridge AS
tagesk@unibridge.no

Noen Unibridge kunder

Post-og teletilsynet

FORSVARET
Forsvarets logistikkorganisasjon

Danske Bank

Nordea

nets

Justis- og beredskaps-departementet

KONGSBERG

STATOIL

BSK Bankenes Standardiseringskontor

bankID

POLITIET

difi Direktoratet for forvaltning og IKT

DNV

UDI

AkerSolutions

Telia

ULLEVÅL universitetssykehus

telenor

NOKIA

buypass securing transactions

NÆRINGS- OG HANDELSDEPARTEMENTET

Statens vegvesen

Oslo kommune

unibridge

Oversikt

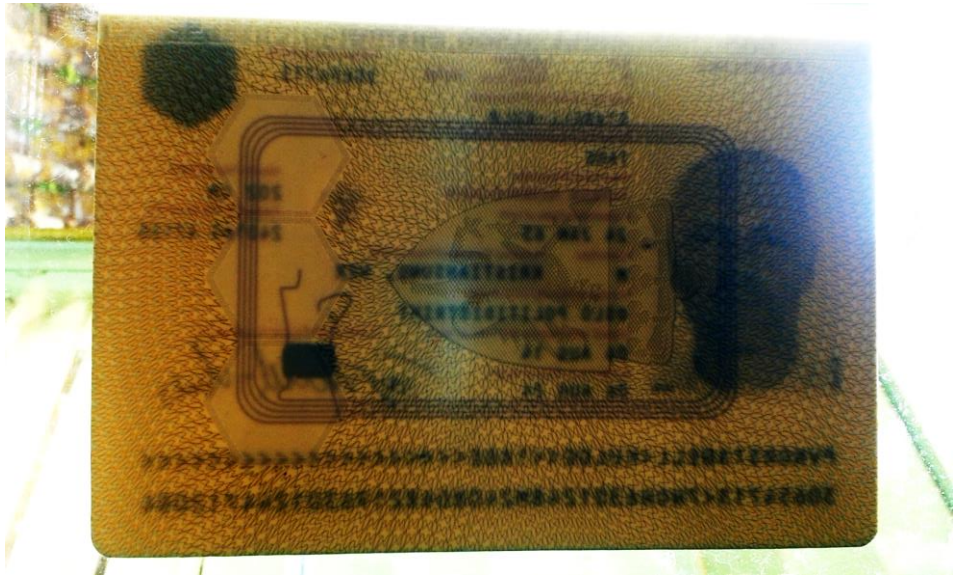
Tre tema som er relevant for pass og ID-kort

- Når kontekst er asymmetriske nøkler

1. Global PKI for verifikasjon av informasjon i pass og ID-kort
   - I regi av FNs luftfartsorganisasjon
   - Egentlig en skog av PKI'er uten sertifisert rot
2. Nasjonal PKI for beskyttelse av fingeravtrykk
3. Mekanisme for etablering av sesjonsnøkler

Pass og ID-kort (dokumentet)

- Innholdet i brikken:
  - «layout» er likt for alle land i verden
    - FNs luftfartsorganisasjon (ICAO 9303)
  - Et sett med datagrupper
    - For eksempel:
      - DG01 er en kopi av det du ser på personaliasiden
  - Et fingeravtrykk («hash») regnes ut over alle data
  - Signaturen på fingeravtrykket lagres i passet



Nøkler (og sertifikater)

- Justisministeren (hans departement)
  - Har generert et nøkkelpar
    - Med innhold (rekkefølge og koding) i tråd med ICAOs spesifikasjon
  - Selv-signert nøkkelparet
  - Nøkkelen heter Country Signing Certification Authority
    - CSCA
    - Kjør «CSCA policy Norway» i Google for å finne policy
  - CSCA genererer
    - Et nøkkelpar
      - Kalles Document Signer (DS)
    - Sertifiserer DS med:
      - Gyldighet 10 år (samme som dokumentene)
      - Brukstid 90 dager
    - Altså:
      - Sertifikatet som gir nøkkelen (DS) verdi er gyldig selv om den ikke kan brukes!

Signering

- Document Signer (DS):
  - Leveres produsenten
  - Installeres i en HSM
    - Hardware Security Module
  - Brukes til å signere innholdet i hvert enkelt dokument
    - I 90 dager
  - Den offentlige nøkkelen legges ned i dokumentet
    - For lokal verifikasjon

Global PKI

- CSCA er personlig levert til ICAO
  - Med brev fra Justisministeren som sertifiserer nøkkelen
- Hver gang en ny DS genereres:
  - Sertifiseres av CSCA
    - Husk bare 90 dagers brukstid
  - Lastes opp til ICAO over nettet
    - Verifiseres mot CSCA som er overlevert
- ICAO legger den ut
  - https://pkddownloadsg.icao.int/
- Alle land gjør det samme
  - Effekt:

    En PKI uten sertifisert rot

Eksempel: Utenlandsk dokument

- Leser:
  - Data
  - Signaturen laget med DS
  - Verifiserer signaturen

- Kontakter ICAO (on-line)
  - Henter CSCA
  - Henter DS med sertifikat fra CSCA
    - Sjekker at DS er sertifisert
  - Konkluderer med at dokumentet
    - Er ekte
    - Ikke er modifisert

Fingeravtrykk

- Justisministeren har
  - Generert et nøkkelpar
    - Country Verifying Certification Authority (CVCA)
  - Selv-sertifisert paret

- Generert et nytt nøkkelpar
  - Document Verification Certification Authority (DVCA)
  - Legges i HSM hos produsenten
    - Brukes til å lage sertifikater som legges inn i brikken i passet
- Brikken forventer:
  - {Les fingeravtrykk}
    - Signert med en nøkkel som har en «link» til DVCA
  - Fingeravtrykkene er altså ikke kryptert, men beskyttet i brikken

- Norge kan levere en nøkkel til et annet land
  - Er så vidt jeg vet aldri gjort

Sammendrag

- Country Signing Certification Authority (CSCA)
  - Lastet opp i en global katalog
  - Blir PKI uten sertifisert rot
  - Signerer en Document Signer…
    - …som signerer innholdet i dokumenter
- Country Verification Certification Authority (CVCA)
  - Signerer en DS….
    - ….som brukes til å fortelle brikken hva den skal kreve
- Utlesing av fingeravtrykk krever altså:
  - Sertifikatkjede fra CVCA
  - Som (i praksis) krever Elliptiske Kurver (!)


unibridge