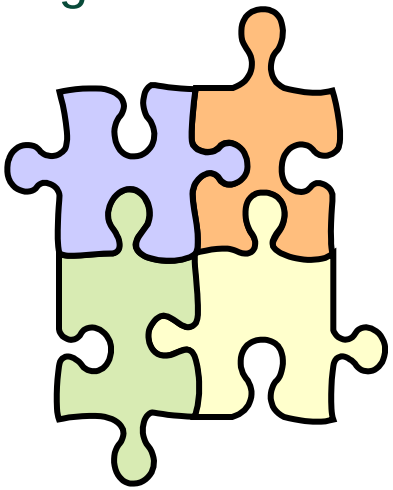
BankID

UNIK - Academic Forum on Security

Invitert presentasjon: BankID - noen myter og sannheer

August 2008



Kontekst: BankID og BSK

BSK: = Bankenes Standardiseringskontor

Etablert 1994 på bakgrunn av avtale mellom de to bankforeninger

Forvaltningsoppgaver knyttet til betalings- og informasjonsformidling i bankenes infrastruktur.

- Standarder
- Meldingsformater
- Sikkerhetspolicyer
- Sikkerhetskrav

Vedtak i BSK er forpliktende for bankene. Har sanksjonsmuligheter.

BankID Samarbeidet:

Etablert av de to bankforeninger.

- I praksis er Fellesutvalg for Betalingsformidling det besluttende organ.

Arbeid gjøres i arbeidsgrupper som ledes av en ansatt koordinator.

- Har et Fagutvalg som rådgivende organ.
- Faste og temporære arbeidsgrupper settes opp.

BSK har ansvar for teknisk koordinering og setter sikkerhetskrav.

BankID Myter, sannheter og angrep - forhistorie

1998: Banknæringen involveres i Nærings- og Handelsdepartementets utredning: ”Digitale signaturer gir tillit til elektronisk kommunikasjon”.

1999: Banknæringen lager studien ”Sikker Meldingsutveksling i åpne nett”. Her legges premissene for et omfattende banksamarbeid.

2000: Første BankID fellesaktivitet startes med prosj.leder fra Sparebankforeningen.

2001: BankID Koordinator blir ansatt av de to bankforeninger.

2002 (apr): Banklagret nøkkelbærer velges.

2002 (sept): De to bankforeninger gir BBS i oppdrag å utvikle en felles operativ infrastruktur (FOI / eng.COI) for BankID i Norge

BankID – Hvorfor sentrallagret (banklagret) løsning?

Bakgrunn:

DnBs erfaringer med sin nettbank 1999-2001

- Kunder klarer ikke å laste ned og installere programvare.
- Kunder sitter på langsomme linjer.
- Kunder kan ikke motta noe over 100 K.
- Supportkostnadene med installert klientprogram blir ubehagelig høye.

Alternativer:

Sentrallagret løsning med transport og lokal bruk.

Sentrallagret løsning med autentisering og sentral bruk.

Produkterfaring:

Baltimore

Cryptomathic

Banklagret løsning med sentral bruk

- Brukeres passord skal ikke lagres noe sted.
- Brukeres private nøkkel skal ikke være tilgjengelig for operatør eller bank på noe tidspunkt, og aldri forekomme i klartekst utenom HSM.
- Kvalitet og tillit til OTP-device / kodebrikke / engangskodebrikke er helt nødvendig!
- I 2002 hadde de fleste norske banker tatt steget over i to-faktor autentisering og ønsket å gjenbruke det de hadde.
- Bankene ønsket ikke å evaluere hverandres løsninger.
- BSK ble bedt om å gjøre evaluering og støttet seg på uavhengig forskningsinstitutt (Norsk Regnesentral).
  - Fortrykt kodekort som kunne kopieres ble underkjent.
  - Utsendelse av kode via SMS til mobiltelefon ble underkjent.
- I tillegg er det en utfordring i å sikre distribusjon av enhetene og knytning til rettmessig bruker.

Utvikling av banklagret og lokallagret BankID

- Pr. 2004-2005 var trusselbildet for lokallagret BankID (med dobbelkrypterte, softe nøkkelfiler) begynt å bli utrivelig.
- BSK kravdokumenter stilte krav om beskyttelse av brukers PC med anti-virus program, men et slikt krav er umulig å følge opp……
- Flere bankrepresentanter argumenterte med at lokallagret BankID var på vei mot et uakseptabelt sikkerhetsnivå.
- Samling om banklagret løsning for PersonBankID og AnsattBankID.
- Tre typer OTP-devicer finnes p.t. for banklagret BankID:
  - Ulike måter å generere engangskodene på
- BSK godkjenner OTP-devicer og distribusjonsløsninger for 2 år om gangen. Nåværende går ut april 2010.

Noen tanker om trusselbildet:

- Det blir ikke nødvendigvis flere fiender der ute.
- Fiendene blir mer profesjonelle.
  - Det finnes en hel økonomi for omsetning av malware og angrep
- Det blir spredd mer og mer malware.

  - Mange web-sites er i periodevis infisert.
  - Mye går under radaren på anti-virus programmene.
- Allikevel er det ikke mer angrep enn tidligere.
  - Flere land i Europa bekrefter et rolig 1. halvår 2008.
- For mange typer nettbankangrep vil BankID ikke bety noe for trusselbildet.
- BankID og norsk språk gir oss en kortsiktig ”security by obscurity” fordel. I lengden kan vi ikke belage oss på dette.

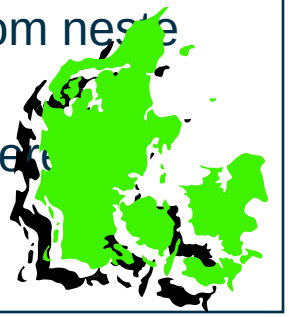
Flere tanker om trusselbildet:

- 2-faktor autentisering:
  - Norske banker var tidlig ute med slik pålogging
  - Ikke like tidlig ute med autentisering av transaksjoner
  - Største delen av europeisk banknæring (inkl. Norge) er nå der.

- Hvor lenge kan nåværende autentiseringsløsninger beholdes - hva kan tenkes å komme etterpå?:
  - Kontekstavhengighet
    - For ulike typer transaksjoner
    - Beregnet over challenge / transaksjonsinnhold
  - Reelle to-kanal løsninger
    - Hvor lenge er kanalene uavhengige?????

Finnes det noen som likner oss?

- Luxembourg:
  - luxtrust.lu: Certificate signing server
  - basert på Cryptomathic-teknologi, utviklet 2005-6
  - ikke rullet ut i volum
  - ingen planer om å registrere seg som kvalifisert sertifikat
  - drift fordelt på to steder
  - bruker har klientprogramvare
- Danmark:
  - PBS (og TDC) har inngått kontrakt med IT- og Telestyrelsen om neste generasjons digitale signatur i Danmark
  - For massemarkedet er dette en sentrallagret løsning der brukere autentiserer seg med kodekort
  - Også nettbankene vil bruke denne løsningen



Kritikk fra akademiske miljøer

- Hole (Bergen) har publisert artikler og påvist en mulig mann-i-midten situasjon (tettet igjen).
- Gjøsteen (NTNU) har publisert flere teoretiske angrep som utnytter mulige svakheter i krypto-håndtering.
- Uttrykt skepsis til modellen med sentrallagret løsning og til banken som tillitsoperatør og tiltrodd tredje part.
- ”No system developed by the banks should be allowed into wide-spread use without rigorous public evaluation by independt experts.”
- Forteller at det er dialog med bankene og at noe av det som er påpekt tidligere, er rettet.

Oppsummering av kritikk

- Å drive sertifikatfabrikk (CA) er ”enkelt”.
- Å registrere og utruste millioner av kunder er vanskeligere.
- Å distribuere programvare med sikker programvare og ”tillitspunkt” viser seg svært utfordrende.
  - Paper i IEEE Security&Privacy: Robbing banks with their own software.
- Kritikk retter seg mot svakheter i programvare og sikkerhetsprotkoller.
- Vi har en stor mengde av proprietær teknologi i BankID løsningene. Dette viser seg å være større utfordring for å skape tillit enn opprinnelig tenkt.

Status pr nå

- Vi har allerede en stor brukermasse og høyt bruksvolum.
  - 1.5 mill sert er ute + 37 pilotsertifikater på mobiltelefon
  - Både nettbank og eID er i ferd med å bli kritisk infrastruktur i det norske samfunnet
  - Bankenes og kundenes interesser må ivaretas