NSMs kryptoaktiviteter

Norsk kryptoseminar 2007

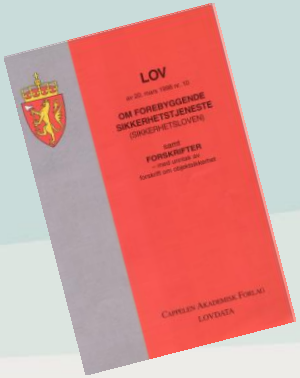
Terje Jensen
Seksjon for kryptoteknologi
terje.jensen@nsm.stat.no
www.nsm.stat.no

Innhold

- Bakgrunn
- Interoperabilitet
- Diskkrypto
- Lavgradert
- Sivile organisasjoner
- Forskning og utvikling
- Ikke-kryptografiske utfordringer
- Kryptografiske utfordringer

Bakgrunn (1/2)

- Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven) regulerer NSMs virke
  - Andre pålagte oppgaver
- Ved kommunikasjon av sikkerhetsgradert informasjon utenfor eget kontrollert område skal det benyttes kryptering og dekryptering
- Kryptering og dekryptering skal bare foretas med kryptoutstyr og metode … godkjent av NSM



Bakgrunn (2/2)

- Kryptoutstyr er tradisjonelt inndelt i to områder:

1. High-grade krypto
   - KONFIDENSIELT, HEMMELIG, STRENGT HEMMELIG
   - Strenge håndteringsregler og krav til brukere

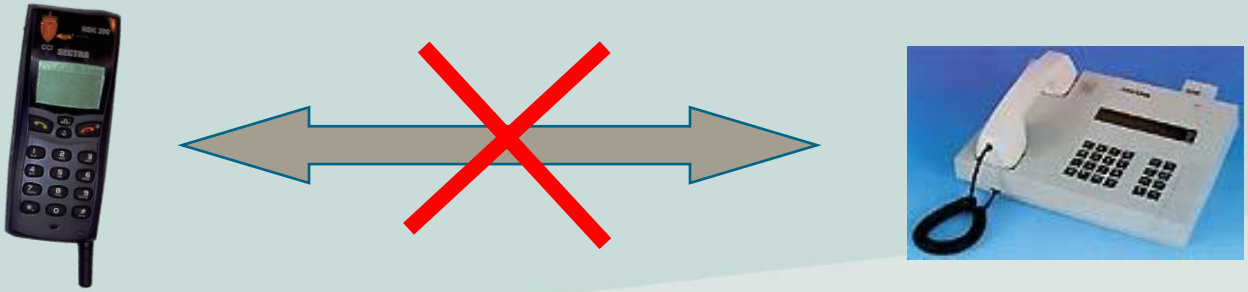
2. Low-grade krypto
   - BEGRENSET, FORTROLIG, STRENGT FORTROLIG
   - Håndteres som verdigjenstander

Interoperabilitet

- Egentlig **sikker** interoperabilitet
  - Kryptoteknologi har vært (og er i stor grad) nasjonale hemmeligheter
- Fokus på interoperabelt utstyr både nasjonalt og internasjonalt
- Internasjonalt, spesielt grunnet internasjonale operasjoner
  - Hver nasjon har sitt eget utstyr
- Nasjonalt, grunnet fokus på enklere utstyr og mer tilgjengelighet
  - Teknologiske utfordringer

Interoperabilitet

- Eksempelvis er det ikke mulig å kommunisere sikkert mellom GSM-systemer og PSTN/ISDN-systemer
- Forskjellige grunner til dette
  - Brukerkrav, teknologi, nøkkelhåndtering



Interoperabilitet

- NSM har to store programmer

1. SCIP
   - Secure Communications Interoperability Protocol
   - Tale og smalbånd data

2. IP
   - Påbegynt aktivitet for å utvikle en NATO-standard
   - Norge er i dag leverandør av IP-kryptoutstyr

Diskkrypto

- Mangler godkjente løsninger for fulldiskkryptering
- Har filkryptoløsning for lavgradert
  - Ønsker ikke å gjenta dette grunnet utfordringer bl.a. rundt operativsystemer
- Flere prosjekter på trappene for både lav- og høygradert
- Gode kommersielle løsninger er tilgjengelige
  - Pågående evalueringsaktiviteter

Lavgradert

- Lavgraderte løsninger har tradisjonelt ikke vært prioritert
- Stadig flere krav og ønsker fra brukere på dette området
  - Både kommunikasjons- og diskkryptoløsninger
- Pågående aktiviteter for å se på rene kommersielle løsninger
- Har publisert kryptografiske krav for lavgraderte løsninger
  - NSM Cryptographic Requirements
  - Baseres på FIPS 140-2
  - Publisert på NSMs hjemmesider

Sivile organisasjoner

- Nødetater, departement og annen sivil administrasjon
- I hovedsak etterspørres lavgraderte løsninger
- ”Nye” utfordringer angående brukervennlighet
  - Tradisjonelle brukere er mer vant til prosedyrer og har lang erfaring
  - Kryptosystemer blir et nytt verktøy for mange
- Enklere administrasjon og bruk, men bevare god sikkerhet
  - Dette vil også gjøre seg gjeldende for tradisjonelle brukere, som ønsker å redusere administrative aktiviteter for personell

Forskning og utvikling

- NSM har flere fagområder med FoU-aktiviteter
  - Interne aktiviteter
  - Benytte industri og forskningsinstitusjoner
    - for å ta frem prototyper, eller belyse/analysere problemstillinger
  - Forsøker å få en mer helhetlig tilnærming
- Planer om å utvide aktiviteter mot universiteter og andre forskningsmiljøer
- På kryptosiden har det vært betydelig aktivitet de senere årene
  - Forventer at dette vil opprettholdes
  - Fokus på ”in-house” aktiviteter

Ikke-kryptografiske utfordringer

- Mye er knyttet til telekommunikasjon, spesielt mobilkommunikasjon
  - Usikkerhet rundt datakommunikasjon i GSM
  - Pakkesvitsjet (i praksis IP) tar over for linjesvitsjet
- Benytter kommersielle nettverk
- Hvilke teknologier/tjenester vil være tilgjengelige når?
  - UMTS, WLAN, standarder for datakommunikasjon i mobile nett
  - Roaming, tjenestekvalitet

Ikke-kryptografiske utfordringer

- Aldrende utstyr må erstattes
  - Teknologisk utvikling, reservedelsproblematikk
- Fokus på sikkerhet på mange områder
  - Design- og utviklingsmetodikk
  - Programmeringsteknikker
- Rask utvikling av kommersiell hardware, også på sikkerhetssiden
  - Gir også softwaremessige utfordringer

Kryptografiske utfordringer

- Benytter mer publiserte algoritmer
  - Ugraderte mekanismer beskytter gradert informasjon
  - Bakgrunn i brukermønster
- Sertifikatbaserte systemer også for høygradert
  - Gir mulighet for enklere administrasjon
- Asymmetriske algoritmer og protokoller
  - I all hovedsak nøkkelutvekslingsprotokoller

Kryptografiske utfordringer

- Nøkkelutvekslingsprotokoller vil være basert på elliptiske kurver
  - Praktiske årsaker, grunnet bit-lengde
  - Interoperabilitet
- Nye elektroniske nøkkelhåndteringssystemer
  - Sertifikatbasert må være elektronisk grunnet lengde
  - Mer automatikk