



NSM

# Nasjonal sikkerhetsmyndighet

**Turid Herland**  
turid.herland@nsm.stat.no  
www.nsm.stat.no

# Nasjonal sikkerhetsmyndighet

- NSM er eit direktorat for forebyggjande defensiv sikkerheit.
- Underlangt Forsvarsdepartementet, med fagleg rapporteringslinje til Justisdepartementet.
- Ca. 130 tilsette.
- Held til på Kolsås og Akershus festning.



# NSM sine oppgaver

- Utøva funksjonen som nasjonal sikkerhetsmyndighet i samsvar med Sikkerhetsloven.
- Andre samfunnsviktige sikkerhetsoppgaver etter pålegg frå Forsvarsdepartementet eller Justisdepartementet:
  - Driva NorCERT og VDI
  - Driva SERTIT
  - Skjerma forsvarsviktige oppfinningar
  - Støtta norsk kryptoindustri

# Sikkerhetsloven

- § 8: ”Nasjonal sikkerhetsmyndighet skal **koordinere de forebyggende sikkerhetstiltak og kontrollere sikkerhetstilstanden**. Nasjonal sikkerhetsmyndighet er også utøvende organ i forholdet til andre land og internasjonale organisasjoner.”
- Dette inkluderer mellom anna:
  - § 9d: ”bidra til at sikkerhetstiltak utvikles, herunder iverksette forskning og utvikling på områder av betydning for forebyggende sikkerhetstjeneste”
  - gje informasjon, råd og rettleiing til verksemder som er omfatta av sikkerhetsloven
  - forestå godkjenning av sikringstiltak
  - gjennomføra sentral personkontroll
  - forestå produksjon, distribusjon og rekneskapsføring av kryptomateriell
  - føra tilsyn med verksemder som er omfatta av sikkerhetsloven

# Fagområde

- Sikkerhetsadministrasjon
- Dokumentsikkerheit
- Personellsikkerheit
- Sikkerheitsklarering
- Internettsikkerheit: trusselbilete, varslng og handtering
- Nettverks- og perimetersikkerheit og penetrasjonstesting
- Applikasjonssikkerheit og systemintegrasjon
- Kryptoteknologi
- Kryptoadministrasjon
- Vern av kompromitterande elektromagnetisk stråling (TEMPEST)
- Tekniske sikkerheitsundersøkingar
- Fysisk sikring

## FoU i NSM

- Tett samarbeid med industri for å utvikla spesialutstyr
  - High-grade kryptoutstyr
  - Måleutstyr for TEMPEST
  - Automatisering av nøkkelproduksjon og –distribusjon
- Eigenutvikling av programvare på NorCERT
- Samarbeid med universitet om studentoppgåver
- Setja ut oppdrag til industri eller forskingsinstitusjonar
- Mindre studie/prosjekt kan foregå internt

# Aktuelle problemstillinger

- Ønsker grundig analyse av og kunnskap om MQV:
  - Samanlikning med andre protokollar, spesielt MTI
  - Teoretisk analyse av sikkerheiten i dei ulike protokollane
  - Implementasjonsmessige aspekt
  - Samanlikna ytelse/hastighet/båndbredde etc.
  - Teoretisk samanlikning av sikkerheiten i dei ulike modia i MQV
  - Sjå på ubesvarte spørsmål i samband med sikkerheiten til MQV, eventuelt også HMQV

# Aktuelle problemstillingar

- Hash-algoritmar har mange ulike bruksområde innan sikkerheit/krypto. Ulike angrep på dei mest brukte hash-algoritmane har dei siste åra funne svakheitar som aukar sannsynet for kollisjonar.
- Kva bruksområde blir påverka av desse angrepa/svakheitane, og i kva bruksområde er sikkerheiten eventuelt upåverka? Finst det bruksområde der desse kollisjonane ikkje er ein trussel/ikkje reduserer sikkerheiten vesentleg?



# Aktuelle problemstillinger – generelt

- Kva angrep finst, og korleis sikra seg mot dei?
  - Krypto
  - Nettverkssikkerheit
  - Operativsystem
  - TEMPEST
- Korleis samla inn og analysera nettverkstrafikk mest effektivt for å oppdaga angrep?