Träffpunkt CC-
Svenskt PP/cPP arbete

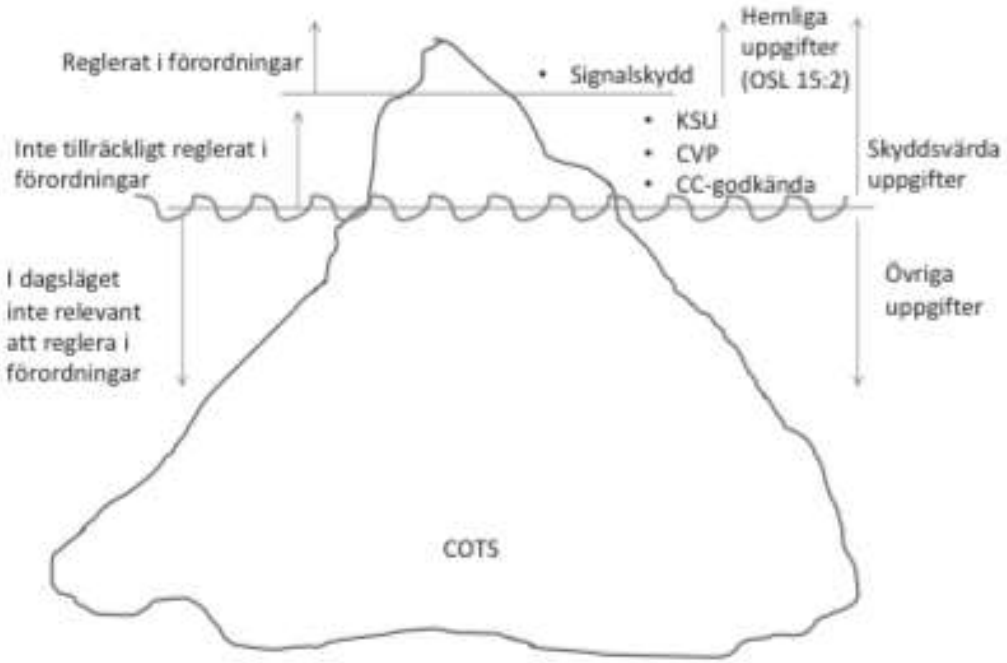
Ronny Janse, MSB

Jan-Ove Larsson, FRA

Bakgrund

- Samhällets behov
- Civilt Försvar
- NISU
  - Bilaga 4 ”Kryptoutredningen”

Klassificerad information (NISU)



Strategi för arbete med standardisering av säkerhet i IT-produkter

Myndigheten för samhällsskydd och beredskap
FÖRSVARSMAKTEN
FMV
Säkerhetspolisen
PTS
FRA
Polisen

Förslag till nationell strategi och åtgärdsplan för säkra kryptografiska funktioner

Förslag till nationell strategi och åtgärdsplan för säkra kryptografiska funktioner – en djupdykning

Bakgrund och problembeskrivning

Förslag till nationell strategi och åtgärdsplan för säkra kryptografiska funktioner – en djupdykning

Hur kan säker kryptering uppnås?

- Säkra kryptografiska algoritmer
- Säkra standarder
- Säkra IT-produkter
- Säkra systemarkitekturer
- Säkra systemimplementationer
- Säker nyckelhantering
- Utbildade användare

Förslag till nationell strategi och åtgärdsplan för säkra kryptografiska funktioner – en djupdykning

Nationellt godkända krypton vs CC-certifierade produkter

Förslag till nationell strategi och åtgärdsplan för säkra kryptografiska funktioner – en djupdykning

Förutsättningar för att lyckas

- Välja rätt kryptering kräver kunskap om teknik och säkerhetspolitik
- En riskbaserad modell
- Kombinationsprincipen
- Standarder för upphandling och reglering

SAMFI-strategi för mobil säkerhet

Behov av mobila tjänster

- Myndigheter har ett behov av att kunna använda *smarta telefoner och surfplattor* för olika informations- och kommunikationstjänster såsom säkert tal, epost, web, dokumenthantering med mera.
- Målet är att skydda information som högst kan vara sekretessbelagd enligt OSL men som ej rör rikets säkerhet.

WYSINWYG

Risker inom mobila området

- Snabb produktutveckling
- Supply chain security
- Stor kodbas; kan inte ha omfattande granskning av appar, OS, FW/HW

Vårt förhållningssätt

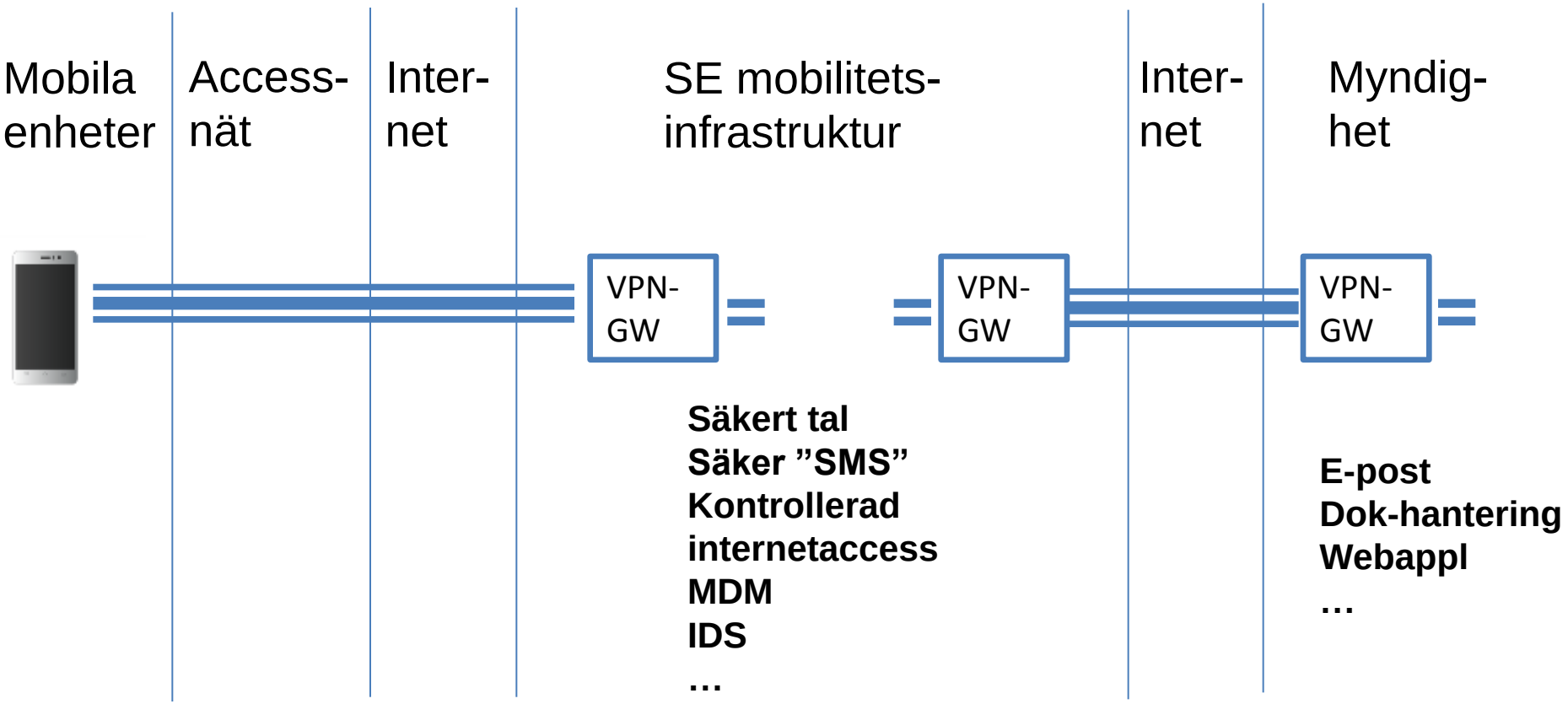
Skydd genom att förebygga, upptäcka, hantera

- Riskbaserat synsätt
- Fokusera på systemsäkerhet i stället för säkerhet i varje enskild komponent
- Arkitektur som nyttjar säkerhet i lager
- Genomtänkt kravställning
- Grundläggande granskning
- MDM och nätverksövervakning
- Incidenthantering inklusive återställning

Tjänster

- Gemensamma tjänster ställer krav på interoperabilitet. Detta kräver att staten tar ansvar för att specificera och tillhandahålla nödvändig infrastruktur.
- Exempel på gemensamma tjänster:
  - Säkert tal
  - Säker ”SMS”
  - Kontrollerad internetaccess
- Exempel på myndighetsspecifika tjänster
  - E-post
  - Dokumenthantering
  - Webapplikationer

Skiss infrastruktur



MSB Myndigheten för samhällsskydd och beredskap
FÖRSVARSMAKTEN
FMV
Säkerhetspolisen
PTS
FRA
Polisen

Krav på mobila enheter

- I kryptoutredningen redovisas en strategi för upphandling och användning av produkter.
- Kommersiella produkter certifierade mot nationellt godkända skyddsprofiler, företrädesvis cPP:er.
- Beroende av infoklassning tillämpas principen om säkerhet i lager , t ex kombinationsprincipen.

Lika konkurrensvillkor för industrin

- Leverantörer ska kunna erbjuda lösningar under lika konkurrens.
- Tydlighet i kravställning och villkor för upphandling.
- Specifikationer av algoritmer, protokoll, gränssnitt och övrig kravställning ska vara tillgängliga för alla potentiella leverantörer.

Skyddsprofiler, prel lista

- Mobile Device Fundamentals
- Mobile OS
- HSM
- HDE
- Network Device PP
    - Extended packages för SIP Server, Firewall, VPN
- Application security
  - MDM
  - VoIP Application
  - Email
  - Web browser

Nationella arbetsformer

- SAMFI
  - AG Skyddsprofiler
  - AG Teknisk
  - Referensgrupp

- Kammarkollegiet
- Informationsspridning

Internationella arbetsformer

- CCRA
  - iTCer
  - ESR
  - cPP
  - position statements
- SOGIS-MRA

Sammanfattning CC-strategi

- Kravställning i form av skyddsprofiler, företrädesvis framtagna i internationell samverkan
- Anvisningar om hur säkerhet i lager ska tillämpas
- Öppna protokoll och gränssnitt som medger att industrin kan ta fram och erbjuda produkter och tjänster
- Algoritmer och protokoll ska i görligaste mån följa internationell standard

Frågor?

Ronny Janse
Ronny.janse@msb.se
Mob: 070-544 75 53

Jan-Ove Larsson
Jan-ove.larsson@fra.se
Tel: 08-471 46 00

Myndigheten för samhällsskydd och beredskap · FÖRSVARSMAKTEN · FMV · Säkerhetspolisen · PTS · FRA · Polisen