

Försvarens utvidgade ansvar inom signalskyddet

Pia Gruvö

chef avdelningen för krypto och it-säkerhet vid MUST

Ny Säkerhetsskyddslag (SFS 2018:585)

Gäller för utövare av säkerhetskänslig verksamhet:

”den som bedriver verksamhet som är av betydelse för Sveriges säkerhet eller omfattar ett internationellt åtagande”

Säkerhetsskyddsklassificerade uppgifter:

”uppgifter som rör säkerhetskänslig verksamhet”

Ny Säkerhetsskyddslag (SFS 2018:585)

Säkerhetsskyddsanalys

Åtgärder:

Informationssäkerhet:

Sekretess, integritet och tillgänglighet

Fysisk säkerhet

Personalsäkerhet

Säkerhetsskyddsklasser

- ✓ Kvalificerat hemlig
- ✓ Hemlig
- ✓ Konfidentiell
- ✓ Begränsat hemlig

Ny Säkerhetsskyddsförordning (SFS 2018:658)

Om säkerhetsskyddsklassificerade uppgifter ska kommuniceras till ett informationssystem utanför verksamhetsutövarens kontroll ska uppgifterna skyddas med *krypto godkänt av Försvarsmakten*.

Försvarsmakten får meddela föreskrifter om krypto för skydd av säkerhetskänslig verksamhet.

Signalskydd

Kryptosystem för skydd av säkerhetskänslig verksamhet benämns signalskyddssystem

- Kryptoapparat
- Kryptonycklar
- Regelverk

Styrkan i signalskyddssystemet anges av signalskyddsgrad (SG)

- "Lägre" nivåer: Restricted (SG R)
- "Högre" nivåer: Secret, TopSecret (SG S, SG TS)
- I många fall även ett intrångsskydd för ett IT-system, ex VPN-krypto

Utveckling

- Försvarsmakten beställer av FMV
- FMV beställer av kryptoindustrin
- Krypto-industrin utvecklar (svensk)
- Vi är med i hela utvecklingsprojektet
- Avslutas med ett godkännande

Vår del

- Algoritm och protokoll
- Nyckelhantering och nyckelproduktion
- Röd-svart separering
- Design
- Hård- och mjukvara
- RÖS-skydd
- "Tamper protection"
- Utvecklingsprocesser
- "Supply chain security"
- Assurans!

Förmågor inom signalskyddet

→ Krypterad datakommunikation

→ SG R

→ SG TS / SG S

→ Meddelandekrypto

→ SG R

→ SG TS / SG S

→ Krypterat tal

→ SG R

→ SG S

Meddelandekrypto SG R

Filkrypto PGBI

Godkänt för Begränsat hemligt, EU Restricted, och NATO Restricted

Mjukvaruapplikation.

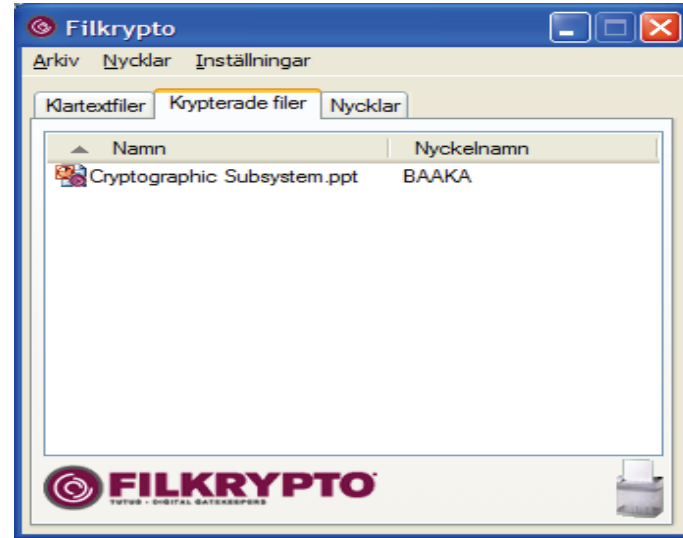
Två varianter - med eller utan nyckelgenerering.

Kryptonycklar kan även beställas centralt.

Klicka och dra fil för kryptering/dekryptering.

Krypterad fil skickas med t ex mail.

Kräver en dator ackrediterad för Begränsat hemlig information.



Projekt Signe

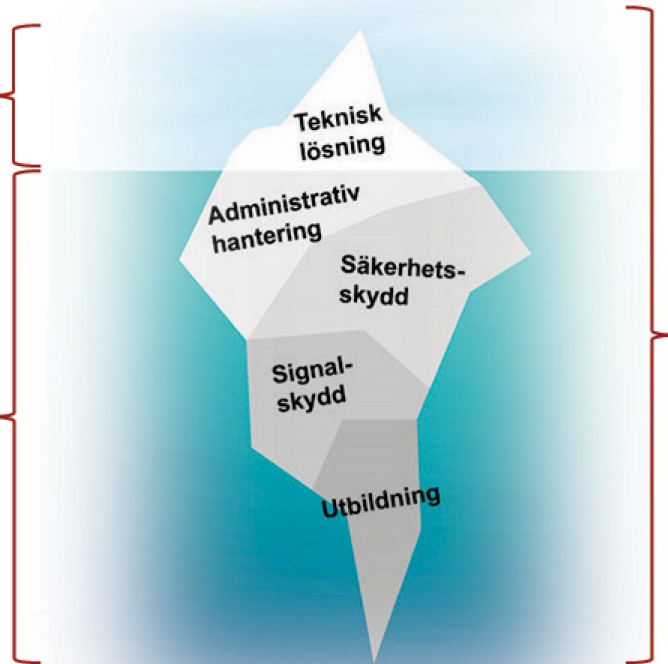
Länsstyrelsen Västra Götalands län

- Projektet syftar till att förstärka
 - länsstyrelsernas **förmåga** att samordna och leda det civila försvaret
 - samarbetspartners **förmåga** att delta i planeringsarbetet av civilt försvar
 - **förmågan** att skydda information av betydelse för totalförsvaret

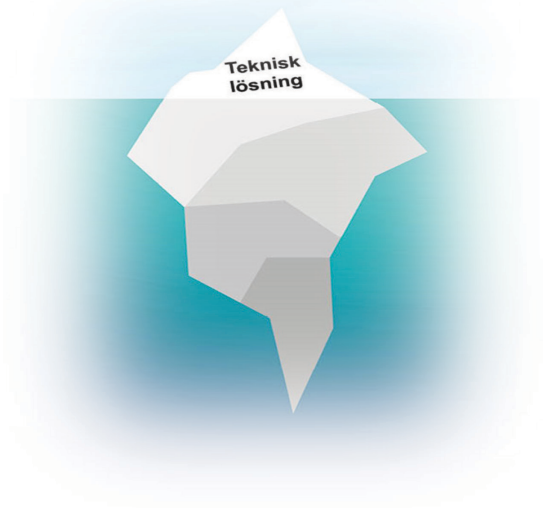
- Projektets förväntade effekt
 - **förmåga** till informationsutbyte av säkerhetsskyddsklassificerad information till nivån **begränsat hemlig**
 - ökad **förmåga** för samtliga samarbetspartners att delta i totalförsvarsplaneringen
 - **förutsättningar** för länsstyrelserna att agera som signalskyddschefer för länens samarbetspartners
 - Anslutna parter har **personal som är utbildade och behöriga** att använda de framtagna kryptolösningarna

Tekniska system

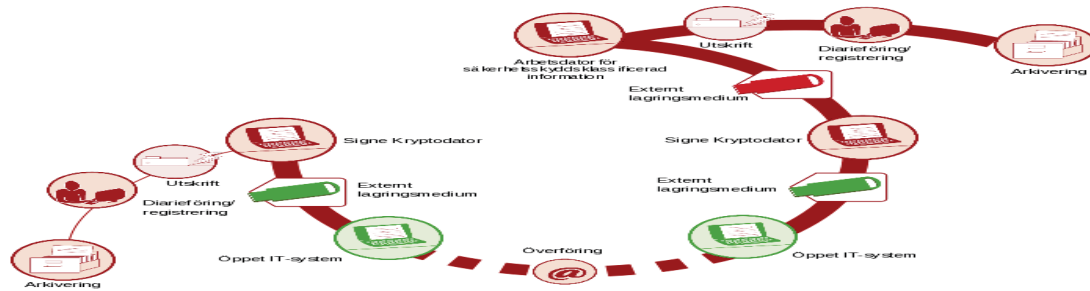
Arbetsformer



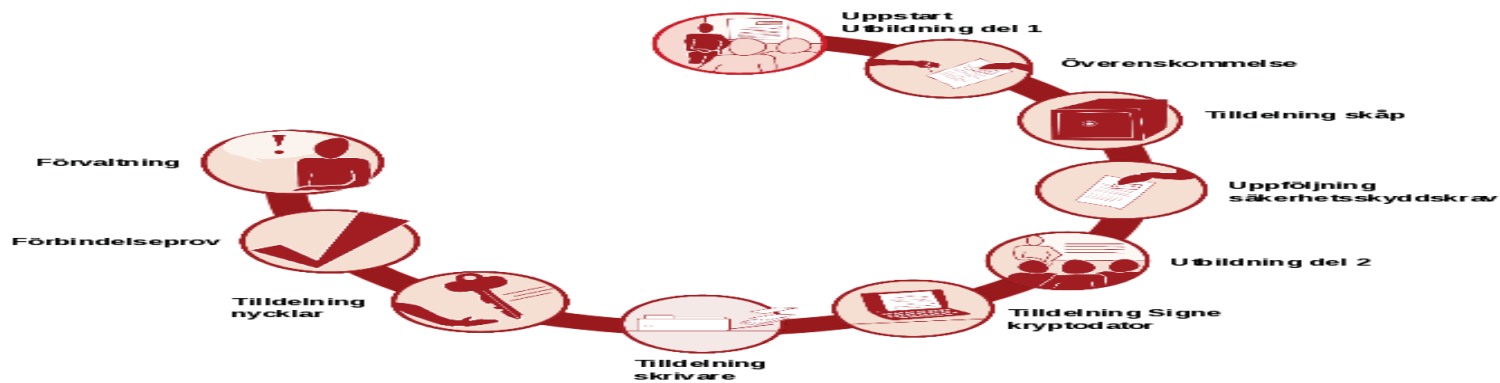
Säker hantering



Signe kryptodator i praktiken



Införande



Länsstyrelsen Västra Götaland

Sambands- och informationssystem inom IT (SIS)



Länsstyrelserna (LST)

Signalskyddschef



Bitr. signalskyddschef & operatörer



Användare



Signalskyddslärare



Säkerhetsskyddschef



Signalskyddsorganisation



Överenskommelse



Delgivning säkerhetsskyddskrav

Samarbetspartners (SP)

Bitr. signalskyddschef & operatör/nyckeladministratör



Användare



Säkerhetsskyddschef



Nuläge

- Signe Kryptodator är under produktion. Under oktober kommer alla Länsstyrelser att få leverans.
- Utbildning av samarbetspartners har börjat och leverans av utrustning kommer att ske från årsskiftet.
- Leveransen består av: säkerhetsskåp, kryptodator, skrivare och optisk enhet.
- Målet är att kunna nå alla 21 Länsstyrelser, 290 kommuner samt 20 regioner via signalskydd (Signe Kryptodator) vid slutet av 2020.
- Förutom ovanstående kommer ett större antal andra samarbetspartners såsom centrala myndigheter/ aktörer, räddningstjänster/ förbund osv.

Övrigt med PGBI

- Nästa generation av ISHV kommer att levereras med PGBI
 - Kompanistabsnivå Q1 2020
 - Bataljonsstabsnivå efter Aurora
- Används idag mellan FMV och Förvarsindustrin
- Begränsad användning i FM
- Andra system för Begränsat hemlig information övervägs
- Andra myndigheter ser över ev införande

- Under övervägande
 - PGBI-PC
 - Ramverk PGBI

Frågor?

