Aktiva kort

Totalförsvarets olika aktiva kort

- Totalförsvaret har en serie av aktiva kort:
  - Totalförsvarets Elektroniska ID-kort (TEID)
  - Totalförsvarets Aktiva kort (TAK)
  - Totalförsvarets Nyckelbärarkort (NBK)
  - Totalförsvarets Databärarkort (DBK)
  - Totalförsvarets Card for Encrypted Keys (CEK)
  - Totalförsvarets Nyckelbärarkort, generation 1 (TAK/NBK) - utgående
- De aktiva korten har olika funktion och användningsområden, men sammanfattningsvis så har de ett eller flera av dessa användningsområden:
  - Identifiering av användare
  - Signering av information
  - Bärare av kryptonycklar och/eller data
- Genom att ange PIN ges åtkomst till de aktiva korten. Efter tre felaktiga PIN låses denna och kan endast låsas upp med upplåsningskoden (PUK), förutom PIN_SIGN som inte kan låsas upp.
- Vid signering kan fingeravtryck (match-on-card) användas som alternativ till PIN för TAK och TEID. Kortterminal 2 (KT2/KT2B/KT2C) är utrustad med fingeravtryckläsare.
- Kort beställs hos lokal kortadministratör. Kort som ska användas av utvecklingsprojekt beställs från FMV:Signalskydd, all utveckling ska ske i samråd med FM MUST SÄKK.
- TAK, NBK, TEID, DBK och CEK är evaluerade i nivå med Common Criteria, EAL 4+. TAK/NBK är evaluerat enligt ITSEC, E4.

v 2.0-081120

Totalförsvarets Elektroniska ID-kort (TEID)

- Användningsområde är främst öppna system och system med informationssäkerhetsklass Restricted (H/R).
- TEID kan jämföras med ett Elektroniskt ID-kort.
- Kortet är tänkt att användas för:
  - Identifiering av användare
  - Signering av information
  - Bärare av data
  - Bärare av kryptonycklar (Signalskyddsgrad SG R)

- TEID är grönt och finns i två utföranden, ID-kort respektive SIM-kort.
- TEID får användas i valfri typ av kortläsare.
- TEID har stöd för biometrisk verifiering.
- TEID innehåller PKCS#15 applet:
  - Innehåller två RSA-nyckelpar med tillhörande användarcertifikat. Det ena nyckelparet används för autentisering och kryptering/dekryptering och det andra för att skapa digitala signaturer.
  - Innehåller ett till två CA-certifikat. Finns det två har dessa olika giltighetstid.
  - Två stycken fingeravtryck kan lagras för access till signeringsnyckeln.
  - Kan lagra kryptonycklar med signalskyddsgrad SG R.

Totalförsvarets Aktiva Kort (TAK)

- Användningsområde är system upp till och med informationssäkerhetsklass Top Secret (H/TS).
- Kortet är tänkt att användas för:
  - Identifiering av användare
  - Signering av information
  - Bärare av kryptonycklar
  - Bärare av data

- TAK är blått och finns endast i ett utförande, ID-kort.
- TAK har stöd för biometrisk verifiering.
- TAK får endast användas i kortterminaler eller kortläsare som har godkänts av Högkvarteret och endast tillsammans med programvaror som är godkända för TAK.
- TAK innehåller två applets:

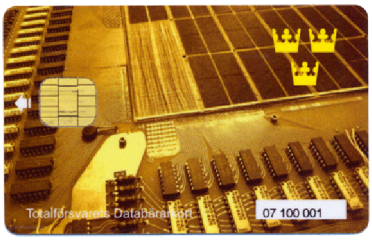
  Applet för PKCS#15:
  - Innehåller två RSA-nyckelpar med tillhörande användarcertifikat. Det ena nyckelparet används för autentisering och kryptering/dekryptering och det andra för att skapa digitala signaturer.
  - Innehåller ett till två CA-certifikat. Finns det två har dessa olika giltighetstid.
  - Två stycken fingeravtryck kan lagras för access till signeringsnyckeln.
  - Kan lagra kryptonycklar med signalskyddsgrad SG R.

  Applet för SKS:
  - Kan lagra symmetriska kryptonycklar upp till och med signalskyddsgrad SG TS.

Totalförsvarets Nyckelbärarkort (NBK)

- Användningsområdet är främst för kryptoutrustning upp till och med signalskyddsgrad SG TS.
- Kortet är tänkt att användas som:
  - Bärare av data
  - Bärare av kryptonycklar
- NBK motsvarar TAK/NBK, men kan innehålla betydligt fler kryptonycklar.
- NBK får endast användas i kortterminaler eller kortläsare som har godkänts av Högkvarteret och endast tillsammans med programvaror som är godkända för NBK.
- NBK är rött och finns i två utföranden, ID-kort respektive SIM-kort.
- NBK innehåller applet för SKS:
  - Kan lagra ett stort antal symmetriska kryptonycklar upp till och med SG TS.
  - Kan lagra godtycklig data.

Databärarkort (DBK)



- Kortet används för lagring av data, exempelvis konfigurationer.
- DBK är gult och finns endast i ett utförande, ID-kort.
- DBK får användas i valfri typ av kortläsare.
- DBK innehåller applet för SKS:
  - Kan lagra ca 40 Kbyte data.

Card for Encrypted Keys (CEK)

- Kortet används för lagring av krypterade nycklar.
- CEK är svart och finns endast i ett utförande, ID-kort.
- CEK får användas i valfri typ av kortläsare.
- CEK innehåller applet för SKS.

Generellt för TEID, TAK, NBK, DBK och CEK

- Korten* består av samma hårdvara och JavaCard plattform:
  - Hårdvara, Philips Semiconductors P5CC072 smart card chip.
  - Plattform, Oberthur Cosmo 64 RSA V5.2 (JMX64R03).
- Korten* är av typ klass A, B och C samt stöder T=0 (transmission protocol)
- Korten har följande Answer-To-Resets (ATR):

TS=3B, T0=1E, TA1=96, T1=80, T2=69, T3=77, T4=E3, T5=03, T6-T9=serienr, T10=01, T12=82, T13=90, T14=00

  - T11=06 för TAK, =0A för TEID, =07 för NBK, =0B för DBK och =1B för CEK.
  - TA1=18 för äldre NBK (se nedan).
  - T10 är =02 för TEID med 2048 bitars publika/privata nycklar.
- *NBK finns också med en äldre version av hårdvara/plattform (P8WE5033, Cosmo 32 V4.0).
  - Detta kort är av typ klass A och B samt stöder T=0.

Hantering och förvaring

(hämtat ur FFS 2005:2)

- Hemlig signalskyddsmateriel samt signalskyddsmateriel, aktiva kort och annan liknande materiel, med inläst kryptonyckel för signalskyddsgrad SG TS, SG S, SG C eller kryptonyckel som är märkt med beteckningen trafikskydd skall stå under ständig uppsikt eller förvaras i ett utrymme som uppfyller lägst kraven för säkerhetsskåp enligt Standardiseringskommissionens normer (SIS), Svensk Standar (SS) 3492.
- Övrig signalskyddsmateriel skall placeras och förvaras så att manipulation och tillgrepp av materielen förhindras.

Publikationer

- I TST AKT 2005, M7446-733103

TEID, TAK, NBK, DBK och CEK:

- Swedish National Defense smart card: SRS applet personalized state, VO Led 12 834:29795/04
- Specifikation avseende ATR mm i aktiva kort, VO Led 12 834:39805/06
- Specification for files for PKCS-applet, VO Led 12 834:54435/2005
- Specification for SKS files, VO Led 12 834:39806/06

TAK/NBK:

- ”Filer i Totalförsvarets aktiva kort TAK/NBK”, Elektro 12 834:38035/98 (utgående)

Tillbehör

Externa kortläsare

- Kortterminal 2 (KT2), M3877-603610
- Kortterminal 2B (KT2B), M3877-603620
- Kortterminal 2C (KT2C), M3877-603640
- Standardläsare av typ PC/SC
- Kryptokort 672/Kryptokort 6721, M3858-672011/M3858-672111

	KK672/ KK6721	KT2	KT2B	KT2C	PC/SC-läsare
TEID	-	X	X	X	X
TAK	-	X[1]	X[1]	X[1]	-
NBK	X	X[2]	X[2]	X[2]	-
DBK	-	-	-	X	X
CEK	-	-	-	X	X
TAK/NBK	-	X	X	X	-

[1] SKS applet endast via kryptokort (KK631/KK6311) [2] Endast via kryptokort (KK631/KK6311)

Övriga kortläsare

- Signalskyddsutrustning utvecklad av Försvarsmakten har vanligtvis inbyggd kortläsare:
  - TAK och NBK stöds i normalfallet
- Kortterminal Administration (KT ADM/KT ADMI), M3877-603520/M3877-603530:
  - Används för att läsa in kryptonycklar och stöder TAK och NBK

Mjukvara

- KrAPI (Krypto API) – Applikationsgränssnitt för kommunikation med de aktiva korten
- PC/SC Drivrutin – Drivrutin för Kortterminal 2/2B/2C