Anvisningar för inloggning i INCA med SITHS-kort

1. Sätt SITHS-kortet i kortläsaren
2. Starta webbläsaren
3. Gå in på INCA
4. Välj certifikat för autentisering (legitimering) och tryck OK
5. Ange din PIN-kod för autentisering (legitimering) och välj ”Jag legitimerar mig”

Vid första inloggningen:

6. Ett meddelande visas:
   ”Det finns ingen användare i INCA kopplad till HSA-identifikationen på ditt SITHS-kort.
   Om du loggar in får du möjlighet att koppla ditt konto till SITHS-kortets HSA-ID”.
   Ange konto (användarnamn) och lösenord som tidigare och tryck på ”Fortsätt”
7. Tryck på knappen ”Associera” för att associera kontot i INCA med det HSA-ID som finns på SITHS-kortet.

Vid påföljande inloggningar behöver endast steg 1-5 utföras

Lyckad inloggning

Efter en lyckad inloggning med hjälp av SITHS-kort måste kortet sitta kvar i kortläsaren under hela sessionen (arbetspasset) med INCA. Tas kortet ut ur kortläsaren kan inte arbetet i INCA fortsätta, det krävs då en ny autentisering och inloggning i INCA.

För att med säkerhet helt avsluta en session och radera information om certifikat och PIN-kod ska webbläsaren stängas av helt efter ett avslutat arbetspass i INCA

Misslyckad inloggning

Om du inte lyckas logga in i INCA med SITHS-kortet

- Ta ut kortet ur kortläsaren. Om inget SITHS-kort finns i kortläsaren övergår INCA under en övergångsperiod automatiskt till svag autentisering med konto och lösenord som är upplagt i INCA. Användare som är registrerade för att använda engångslösenord måste autentisera med engångslösenord om SITHS-kortet inte sitter i kortläsaren.
- Logga in på ”vanligt” sätt.

Alternativet att välja mellan olika typer av autentisering kommer bara att vara möjligt under övergångsperioden när alla användare ännu inte fått sina SITHS-kort.

Användare med flera konton i INCA

En användare som har flera konton i INCA måste associera varje INCA-konto till sitt SITHS-kort .
Låt SITHS-kortet sitta kvar i kortläsaren och välj i menyn under ”Inställningar” menyvalet ”Associera konto med SITHS”. Användaren hamnar då på nytt i INCAs inloggningsprocedur där konto (användarnamn) och lösenord anges. Det nya konto som användaren vill associera med SITHS-kort anges och associeras sedan med HSA-id på SITHS-kortet på samma sätt som tidigare.

När en användare associerat sitt SITHS-kort till flera konton i INCA måste användaren välja ett konto i inloggningsproceduren för att få den auktorisering som passar arbetsuppgiften i INCA. Autentisering är utförd med SITHS-kortet och kontot för auktorisering kan då väljas utan krav på lösenord.

Webbläsare

Med operativsystemet Windows rekommenderas webbläsarna IE9, Firefox eller Chrome
Med operativsystemet Mac OS X rekommenderas endast webbläsare Firefox

Autentisering

Autentisering är en kontroll (verifiering) av uppgiven identitet. I enklaste formen, svag autentisering, sker kontrollen genom att den som identifierar sig, förutom sitt namn, uppger ett personligt lösenord. Stark autentisering används när kravet på säkerhet är högre. Kontroll av uppgiven identitet med engångslösenord eller elektroniskt kort med certifikat för legitimering (SITHS-kort) är exempel på stark autentisering.

Auktorisering

Auktorisering ger en användare rättighet (behörighet) att komma åt viss information och rättighet att göra vissa saker, exempelvis att läsa, ändra, radera och kopiera viss information. Rättigheter i INCA är baserade på roll och placering. Användare i INCA tilldelas en eller flera roller och en eller flera placeringar. En användare väljer en roll och placering som passar för en arbetsuppgift och blir då auktoriserad med vissa rättigheter

Inloggning i INCA = Autentisering + Auktorisering

En användare som loggar in i INCA måste först autentisera sig och sedan bli auktoriserad med de rättigheter som är nödvändiga för att utföra sina arbetsuppgifter