SITHS inloggning i AD

Inloggning med grafiskt gränssnitt kräver Windows 7 eller Vista
Med PassThrough Gina for Windows och NetID version 5.5.0.27

För att logga in i en Windows domän med hjälp av SITHS-kort och certifikat behöver domänen och AD innehållet konfigureras för att hantera certifikat/smartcard inloggningar. HCC specifikation version 2.35 anger de rätta förutsättningarna. Om organisationen matar in data i attributet userPrincipalName, så får kommande SITHS certifikat AD-egenskapen ”smartCardlogon” (ligger i attributet ”enhancedKeyUsage”), vilket krävs för AD-inloggning.

Förutsättningar:
Denna instruktion utgår ifrån att en klient med en fungerande NetID installation och ett aktivt SITHS-kort finns att tillgå. Instruktionen förutsätter också att läsaren är väl förtrogen med Microsoft AD och administrationen av denna.

För att kunna autentisera en användare via ett SITHS smartcard måste Active Directory konfigureras för att hantera och lita på SITHS CA, och på certifikat utfärdade av denna CA.

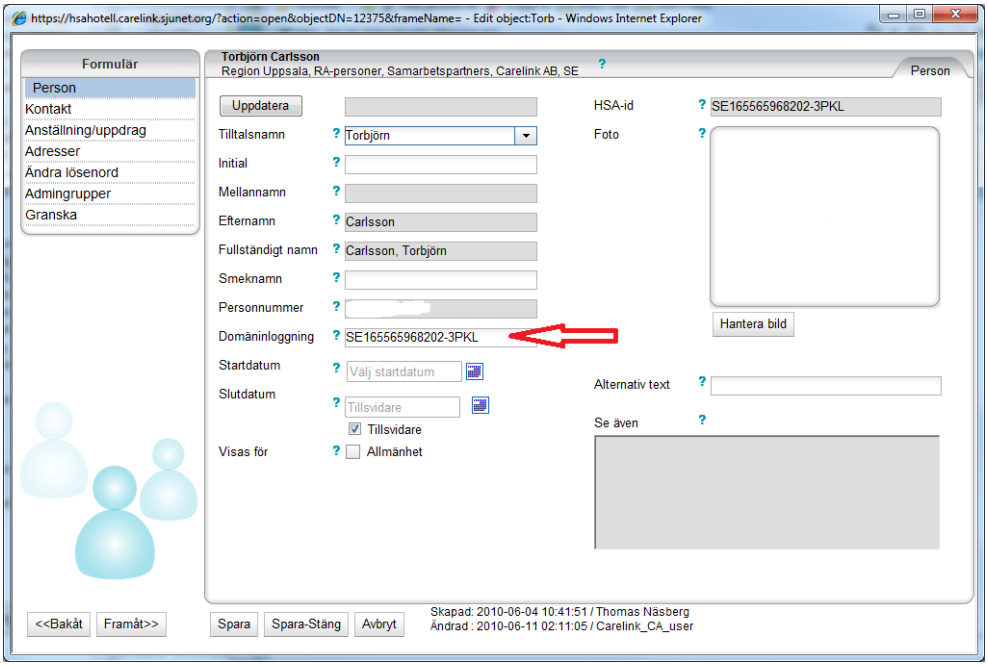
En klientinloggning sker därefter med det ID begrepp som HSA definierat.

Grundinstallation i AD

Som förberedande åtgärder innan SITHS korten kan kopplas till ett användarkonto i AD behöver installationer och konfigurationer av CA-certifikat, servercertifikat och några konfigurationer göras. Dessa beskriv nedan i ordningsföljd.

Förutsättningar

- Domän och servernamnet är bestämt
- Servern har installerats och konfigurerats med AD-rollen
- Microsoft CA är installerad och konfigurerad.
- HSA-katalogens data för användarna är konfigurerade med UPN (Domäninloggning), så att de certifikat som läggs på SITHS kortet skall få rätt fält ifyllda. Se bild nedan från HSA-Admins webgränssnitt.



- Användarnas inloggningsnamn i domänen är eller ändras till HSA-ID (exemplet visar TSE165565594230-0003@siths.inera.se).

Vad ska ske

- SITHS rootcertifikat skall installeras i rätt Cert-store
- AD konfigureras för att automatiskt distribuera SITHS CA-certifikat till klienternas Trusted Root CA store via en AD Group Policy
- Domänkontrollanterna skall ha ett SITHS CA certifikat installerat i sitt NTAuth store.
- Alla domänkontrollanterna som skall hantera klienter skall förses med ett Domain-Controller certifikat för att autentisera smartcard användare.
- Certifikatens UPN skall stämma med AD domän suffix.
- Lägga till användare eller modifiera existerande användares inloggninginformation
- Testa och verifiera inloggning och revokeringskontroller

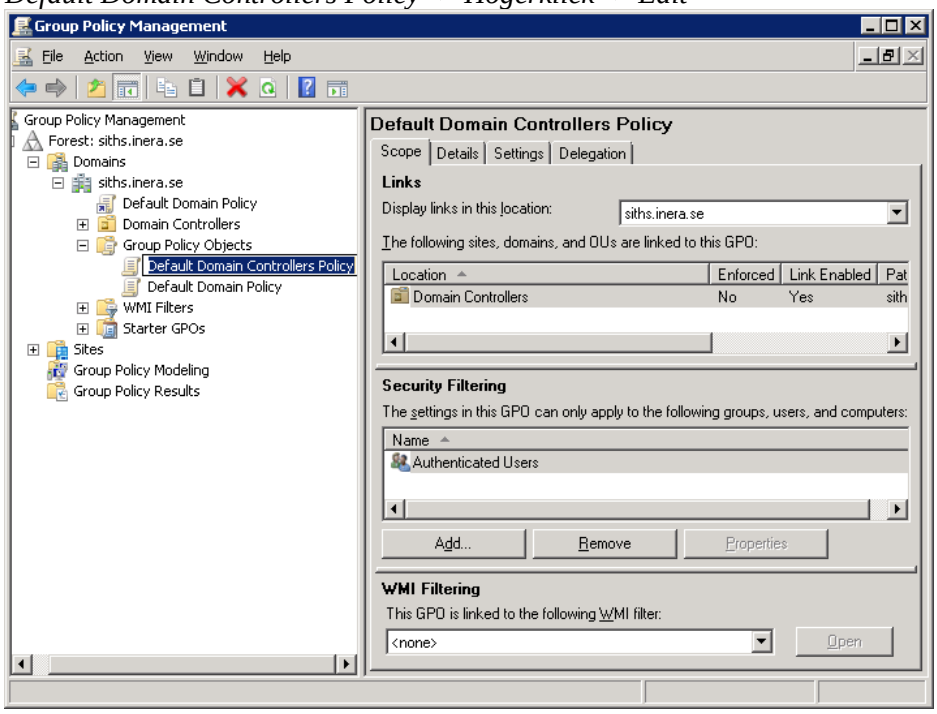
Installera Rootcertifikat

För att SITHS kort skall accepteras av domänen behöver SITHS CA-certifikat vara betrott i domänen.

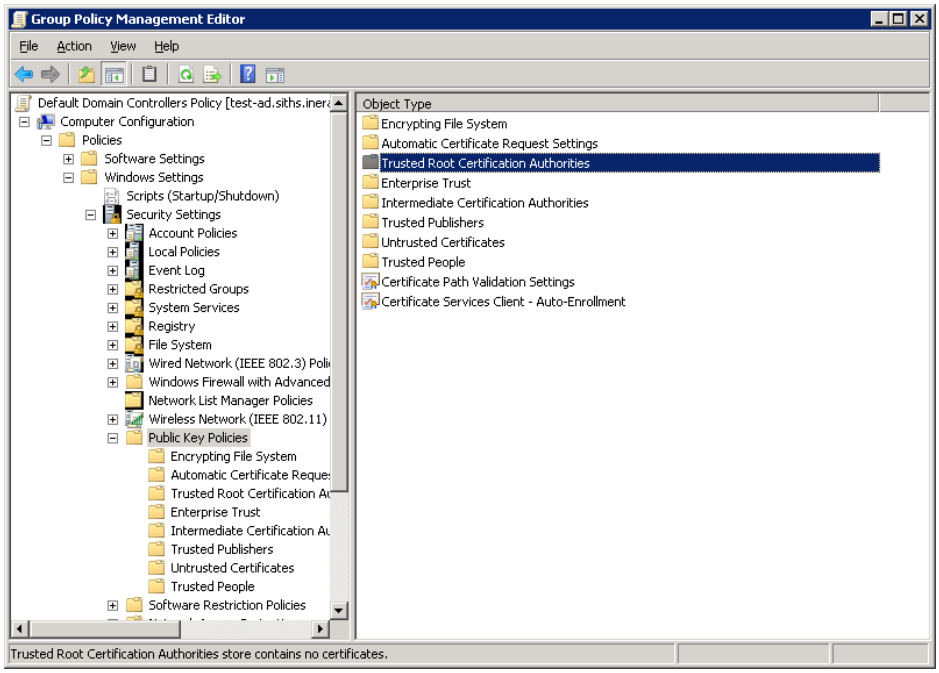
Detta kan göras manuellt per maskin, eller för hela domänen via en Grupp-policy (GPO). I denna beskrivning görs detta via en GPO.

1. Plocka fram ett SITHS CA certifikat kodat i Base64 format

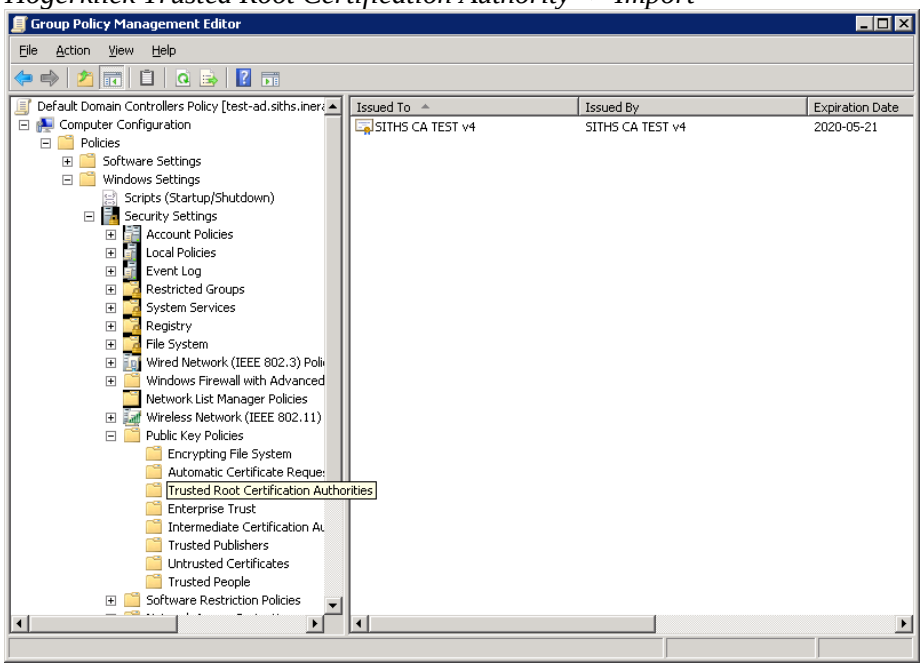
2. Lägg till certifikatet som trusted root i Active Directorys GPO *Default Domain Policy Group Policy -> Trusted Root Certification Authorities*
    a. *Start -> Administrative Tools -> Group Policy Management*
    b. *Expandera domänen & Group Policy Object*
    c. *Default Domain Controllers Policy -> Högerklick -> Edit*



d. *Expandera Policies -> Windows Settings -> Security Settings -> Public Key Policies*



e. *Högerklick Trusted Root Certification Authority -> Import*



f. *Next …. Finish.*

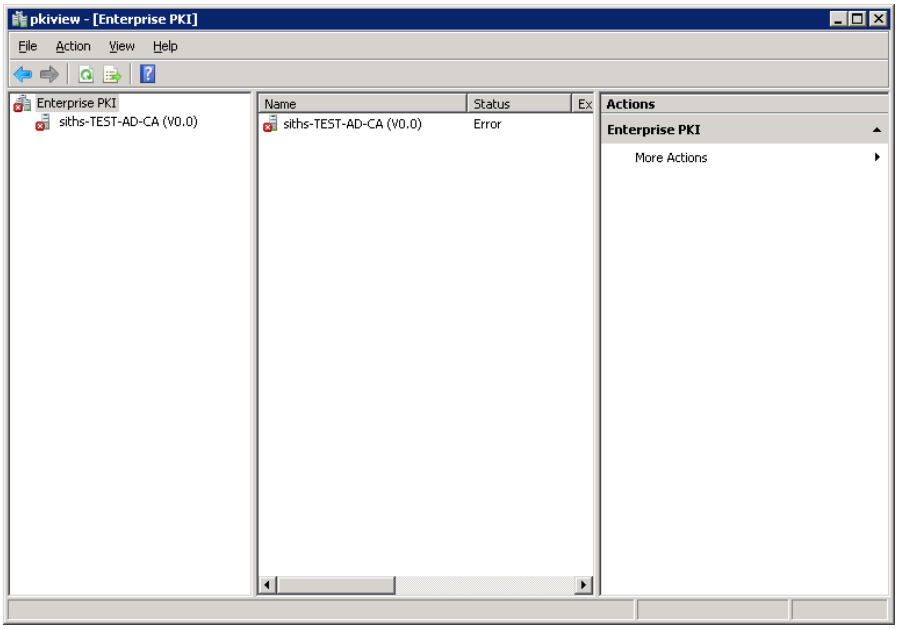
NTAuth CA

För att SITHS certifikaten skall kunna användas i domänen måste även SITHS CA-certifikat finnas med i domänens NTAuth store.

OBS! Detta måste göras för alla domänkontrollanter i domänen.

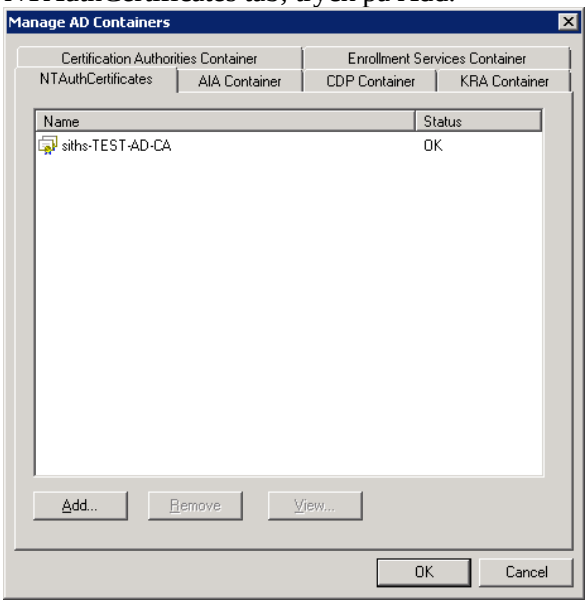
NTAuth store finns inte automatiskt i en grundinstallerad Windows 2008 server utan måstes skapas. Detta kan göras antingen för hand, eller så skapas det automatiskt som en bieffekt av att rollen Microsoft CA läggs till.

1. Installera Microsoft CA rollen.
   OBS! Detta måste planeras då de rootcertifikat mm. som skapas inte på något enkelt sätt kan förändras i efterskott.
2. NTAuth store skapas automatiskt när Microsoft CA installeras, och nås enklast via Start -> Run -> PKIview.msc

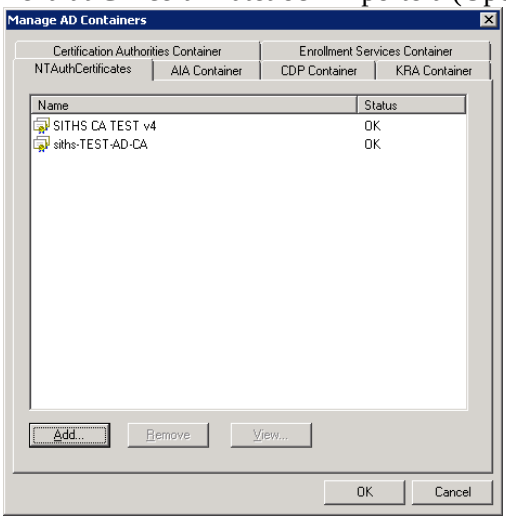


3. Högerklick Enterprise PKI -> Manage AD Containers.

4. NTAuthCertificates tab, tryck på Add.



5. Peka ut CA certifikatet och importera (Open).



Domänens servercertifikat

För att systemet skall hantera en kortbaserad inloggning måste all domänkontrollanter ha egna servercertifikat.

1. Om en Microsoft Enterprise CA finns installerad kan alla DC automatiskt hämtat ett certifikat från denna, och inga extra åtgärder behövs.
2. Om SITHS CA skall användas även för DC servercertifikat:
    a. Beställ certifikat till de domänkontrollanter som finns i domänen och verifiera att dessa certifikat innehåller rätt extensions (Se ref. 3)
    b. Installera certifikat på varje DC. (Se Ref 1 för instruktioner)

Certifikathantering/SmartCard

Det data som finns lagrat i användarens certifikat under "Subject Alternate Name" är det data som kommer att användas som användarens ID (användarnamn) vid inloggning i domänen. Innehållet i AD och på certifikatet måste därför vara lika för att inloggningen skall lyckas. Verifiera därför detta!

Ett korrekt utformat UPN skall följa HSA:s rekommendationer för att fungera i en AD-miljö.

Format: <HSA-ID>@<AD-domän>

Exempel: TSE165565594230-0003@siths.inera.se

Detta kan hanteras på olika sätt beroende på om det är en nyinstallation av domänen, eller om certifikatinloggningen är ett tillägg till en redan existerande infrastruktur.

Existerande domän

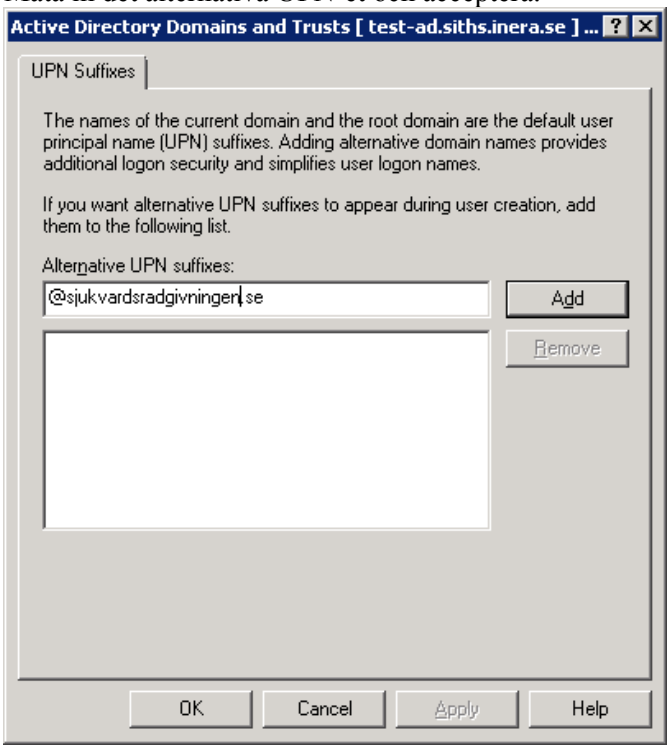
I ett AD som inte har samma UPN-suffix som den som finns i användarnas certifikat, måste AD't uppdateras med certifikatsuffixet. Detta görs genom att lägga till ett alternativt UPN suffix i AD:s Domains and Trusts.

UPN

Ett alternativt UPN suffix läggs till i AD:t genom att

1. Gå in i "Active Directory Domains and Trusts"
2. Markera översta nivån på trädet, högerklick, properties.

3. Mata in det alternativa UPN'et och acceptera.

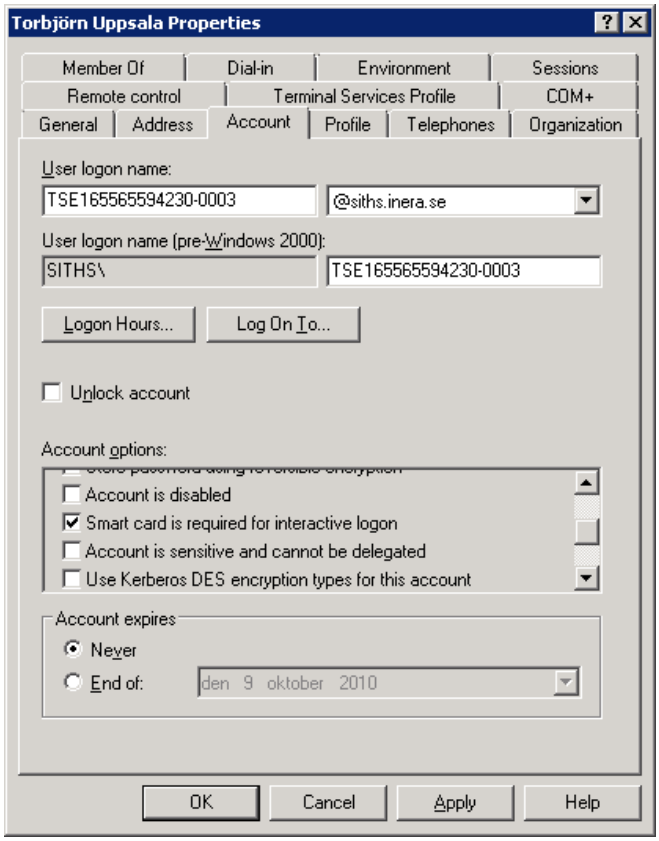


Skapa användare

Gå in i "Active Directory Users and Computers", och skapa en användare.

Användarens login namn (User logon name) skall vara HSA-ID. Det UPN-suffix som finns i certifikatet skall vara valt i dropdown boxen till höger om User logon name.

Under användarens profil kan man även sätta en flagga för att kräva smartcard login för kontot.



Redan existerande användare

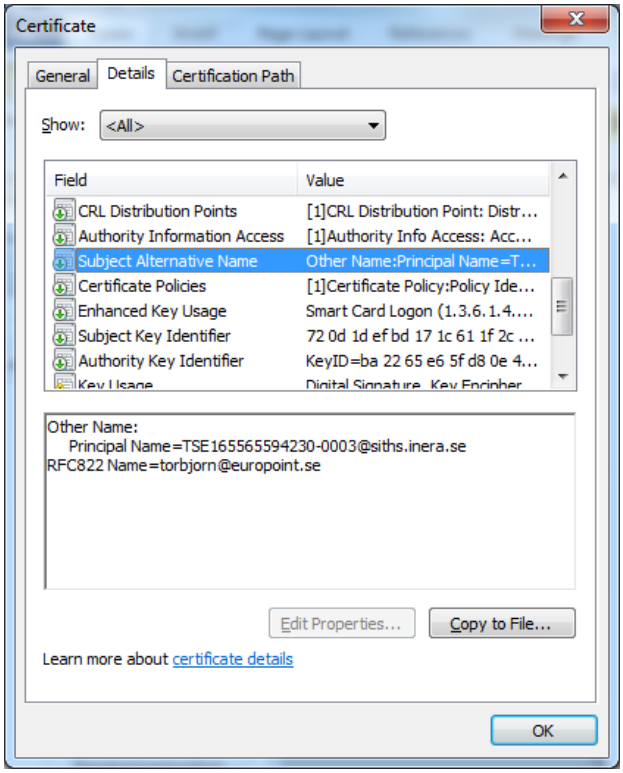
Användare som redan finns i katalogen, och som skall uppgraderas till smartcard-användare måste förändras så att villkoren för kortanvändningen uppfylls.

Detta kan göras på två olika sätt

1. Skapa en ny användare och flytta över den gamla användarens ägarskap och privilegier till den nya profilen.
2. Byt User logon name till HSA-ID med tillhörande korrekta suffix.

Lösning 2 har testats av det pilotprojekt som SLL genomfört, och enligt rapporter från det projektet har inga problem upptäckts vid en sådan förändring.

Verfiera certifikatet



Verifiera att användarens certifikat innehåller ”Subject Aternate Name” fältet i SITHS-certifikatet och att det har samma namn-information (SITHS ID) som användaren har i AD’t.

OBS! Dessa fält måste matcha för att användaren skall kunna logga in.

Användaren kan nu logga in med hjälp av sitt smarta kort.

Klienthantering/Gruppolicys

Automatisk Utloggning eller skärmlåsning

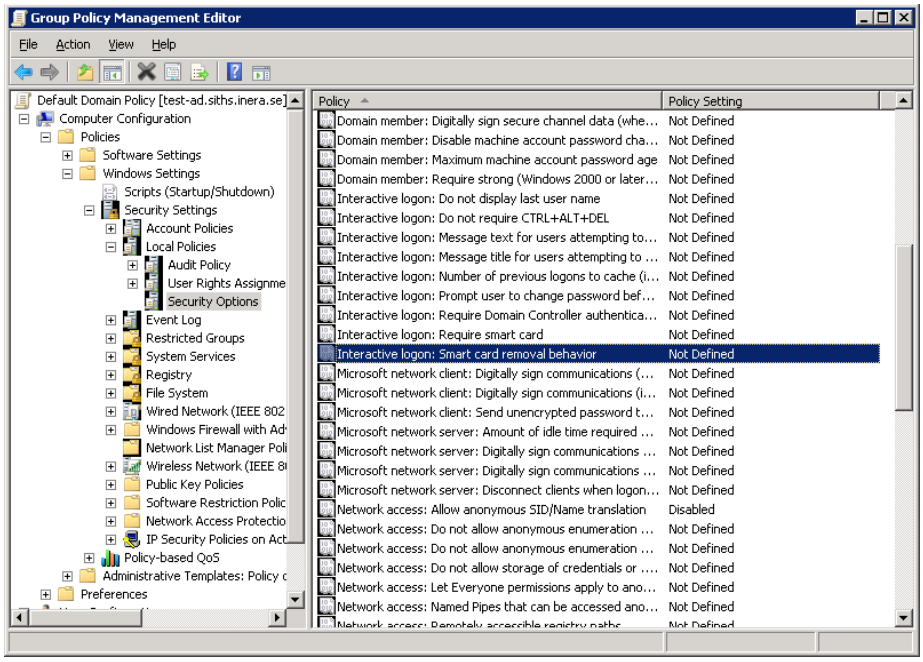
För att låsa skärmen eller logga ut användaren automatiskt när kortet dras ur kortläsaren skall följande policy konfigureras:

GPO: Policies\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behaviour

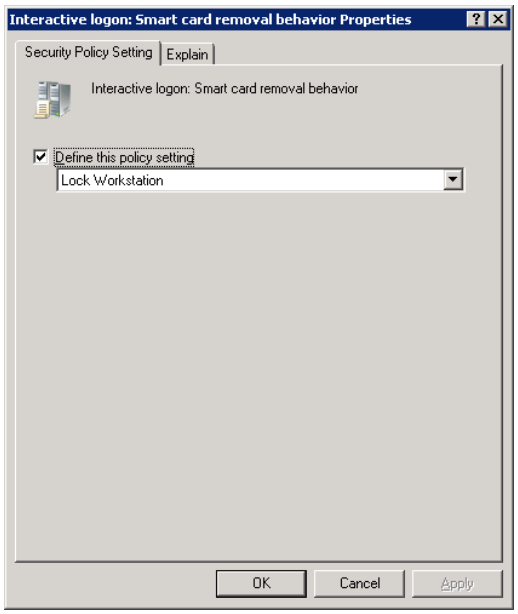
Möjliga inställningar för denna GPO är:

- No Action
- Lock Workstation
- Force Logoff

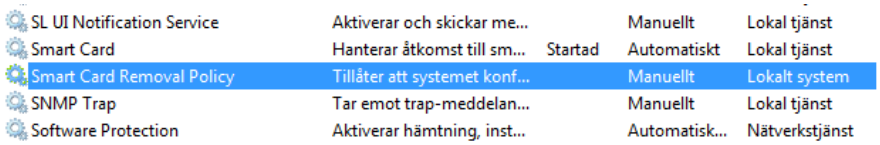
- Disconnect if a remote Terminal Services session



I detta exempel används Lock Workstation som policy för domänen.



Nästa steg är att starta den tjänst som hanterar GPO policyn i klienten:



Tjänsten ”Smart Card Removal Policy” behöver startas för att systemet skall reagera på att man drar ut kortet. Tjänsten måste startas automatiskt på alla klienter för att utloggnings/lås-funktionen skall fungera som avsett.

OBS! Denna tjänst är ny för Windows 7, i tidigare generationers klienter (XP) hanteras detta utan en specifik klienttjänst.

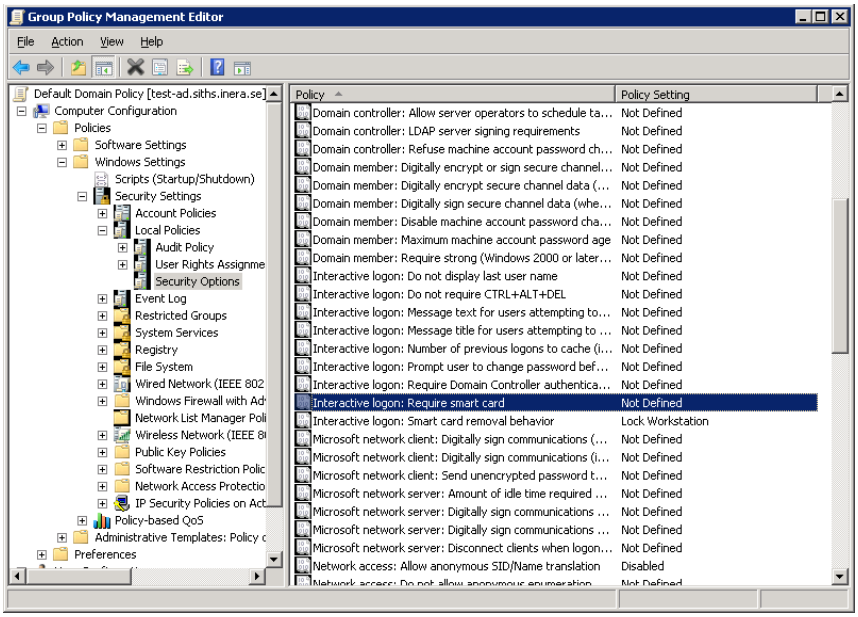
Krav på inloggning med smartcard

Det finns även ett attribut för att åstadkomma en tvingande inloggning med smartcard, men denna inställning skall man nog vara lite försiktig med då risken att låsa sig själv ute är överhängande, men för en produktionsmiljö med höga säkerhetskrav kan denna inställning vara att rekommendera.

För att använda funktionen skall följande policy konfigureras:

GPO: Policies\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Require smart card

- Enabled
- Disabled

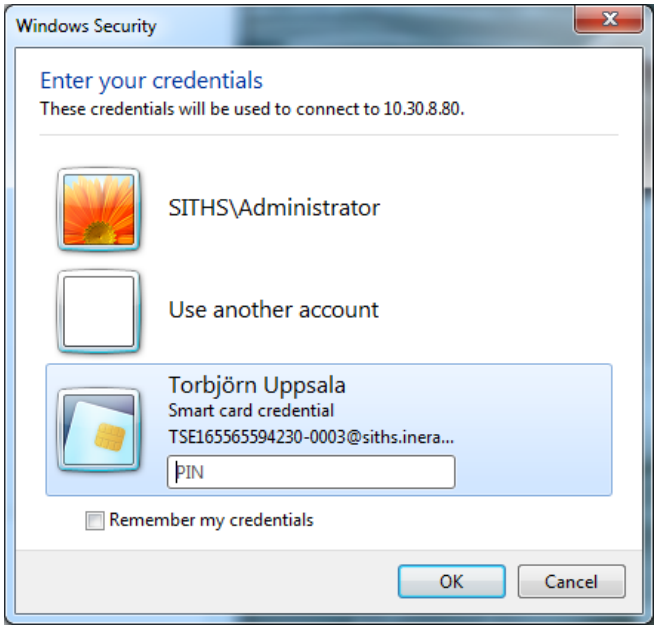


Autentisering av användare

Windowsinloggning Windows 7

För Windows 7 kommer det certifikat som matchar de kriterier som är uppsatta i AD't att presenteras som inloggningsbild.

Även vid en fjärrinloggning via remote desktop kan inloggningen hantera smartcards med en lokal kortläsare.



Windowsinloggning XP

För Windows XP kommer inte certifikaten att presenteras på samma intuitiva sätt. XP presenterar ingen lista på de certifikat som finns att tillgå. I det vanligaste fallet med endast ett giltigt certifikat på kortet visas en PIN-kods dialog upp för användaren som där anger sin PIN och blir inloggad.

Det är dock besvärligare att använda kort med flera installerade certifikat, då sättet att välja vilket certifikat som skall användas är svårhanterligt.

Detta fenomen har NetID/SecMaker utrett, och för närmare instruktioner för multipla certifikat och Windows XP hänvisas till de dokument som Secmaker publicerat.

Revokeringskontroller

Kontrollera att AD och DC verifierar mot SITHS CRL'er i HSA

För att verifiera att revokeringskontroller görs kan man titta i EventManagern.

1. Öppna Applications and Service Logs -> Microsoft -> Windows -> CAPI2
2. Högerklick på Operational
3. Välj "Enable Log"
4. Logga in via SmartCard och NetID
5. Högerklick på Operational -> Refresh
6. Dubbelklick på eventid 40 & 41 och välj fliken Details
7. Titta på RevocationStatus.