Krav och rekommendationer på klientplattformen

Innehållsförteckning

1 Versioner

Version	Datum	Beskrivning	Upprättat av
1.0	2012-12-17	Dokument upprättat.	Jim Larsson
1.1	2014-04-03	Uppdatering gällande publika sidan	David Landerborn

2 Revisioner

Avsnitt	Datum	Beskrivning	Upprättat av
6.2	2015-12-10	Förklaring av tillgängligt minne tillagd	Mats Persson
6.10	2015-12-10	Tillägg rekommendation då man har både trådad och trådlös förbindelse	Mats Persson
6.11	2015-12-10	Sänkning av krav då flera användare delar internetförbindelse	Mats Persson

3 Inledning

Pulsen combine är avsett att användas av tre olika användarkategorier. Myndighet, utförare och medborgare. Pulsen combine har tre olika vyer, Myndighetsvy, Utförarvy och Medborgarvy för att motsvara dessa olika användargrupper. Vid referens till de tre vyerna i text i detta dokument är det dessa delar som avser. Lösningen ställer i stort sett samma krav på användarens dator för myndighets och utförardel. Medborgardelen skiljer sig genom att inte ha krav på Silverlight.

4 Aktualitet

Detta dokument beskriver klientkraven för version 1.13 av Pulsen combine.

5 Klientsäkerhet

Pulsen combine har ingen funktionalitet för att säkerställa klientens säkerhetsmässiga tillstånd. Det är upp till varje enskild användare eller dennes organisation att se till att klienten är försedd med lämpligt skydd mot skadlig kod, virus och andra hot. Klientdatorer bör vara patchade för att undvika säkerhetsbrister i operativsystem, vara utrustade med antivirus och skydd mot trojaner.

6 Krav på klient

Pulsen rekommenderar att Pulsen combine körs på en fysisk klientdator med nedan specifikation som lägsta nivå. Pulsen combine kan köras på tunn klient men det har i vissa fall påvisats försämrad prestanda i en sådan lösning.

6.1 Skärmupplösning

Lägsta skärmupplösning för Pulsen combine är 1024x768 bildpunkter. Högre skärmupplösning rekommenderas, t ex 1440x800 eller 1600x1024.

6.2 Primärminne

För Pulsen combine rekommenderas 4 Gbyte tillgängligt minne. Om andra applikationer körs samtidigt är tillgängligt minne det minne som inte används av dessa andra applikationer.

6.3 Processor

Processorn skall uppnå index 5 med hjälp av Microsoft's mätning av performance index på klienten på en Windows 7 maskin.

6.4 Silverlight

Myndighets och utförardelen av Pulsen combine kräver Microsoft Silverlight. Medborgardelen behöver inte Silverlight.

Version: 5.1 32 bitar eller senare

6.5 Operativsystem

Myndighets- och utförarvyn har krav på att användarna kör på av Microsoft supportad version av Windows. För Medborgarvyn supportas även av Apple supportade versioner av MacOS.

6.6 Webbläsare

Pulsen combine har full funktion endast med 32 bitars browsers. Funktionstest genomförs med respektive browser uppsatt med defaultinställningar. Görs avsteg från browserns default-inställningar kan detta medföra att Pulsen combine inte fungerar. Innan ändring av browserinställningar görs bör därför test ske i kontrollerad miljö för att avgöra om ändringarna påverkar möjligheten att köra Pulsen combine.

Microsoft Internet Explorer version 8 eller senare 32 bitar
Mozilla Firefox version 3.6.3 eller senare

6.7 PDF läsare

Medborgar-, Myndighets- och Utförartjänsterna har alla krav på att Acrobat Reader finns installerad. Gällande vilken version av Acrobat Reader som skall användas, hänvisas till rekommendationer för den browser som skall användas

6.8 Net iD

Kunder som kör Pulsen Combine och vill logga in med SITHS-kort behöver förutom kort och kortläsare även programvaran Net iD. Ingen särskild anpassning krävs i Net iD för att kunna logga in i Pulsen combine. Man kan med fördel använda något av de paket som finns tillgängliga för SITHS-kunder. Detta gäller alla tre vyerna av Pulsen combine.

6.9 E-legitimation

För att kunna logga in med olika E-legitimationer behövs en CSP (certificate service provider) Det är en programvara som erhålls av respektive E-legitimationsutfärdare. Installation och konfiguration av denna ligger utanför Pulsen combine.

6.10 Nätverk

Det är rekommenderat att klientdatorn är ansluten med trådad nätverksförbindelse. Pulsen combine kan köras med trådlös förbindelse men detta kan ha negativ påverkan på prestanda och tillgänglighet. Om man har både en trådad och en trådlös förbindelse är det rekommenderat att stänga av den trådlösa förbindelsen då man är uppkopplad mot den trådade förbindelsen, för att undvika problem med anslutningen. När det gäller medborgarsidan finns inga krav på trådad förbindelse.

6.11 Internetförbindelse

Rekommenderad nivå för anslutning mot internet är 10 Mbit/s för myndighets- och utförartjänsten. Delar flera användare på samma internetanslutning rekommenderas 1Mbit/s per användare utöver detta. Lägre anslutning kan påverka prestandan i tjänsten negativt. Medborgarsidan kräver minst 1 Mbit/s.

7 Utloggning

Den enskilde användaren av Pulsen combine ansvarar själv för att logga ut ur Pulsen combine. Utloggning sker endast med ”Logga ut” knappen i användargränssnittet.

7.1 Utdragning av SITHS kort

Utloggning ur Pulsen combine sker alltid med ”Logga ut” knappen i användargränssnittet. Det finns dock möjlighet att låta SecMakers Net iD agera när ett smartkort dras ur kortläsaren. Detta ligger dock helt utanför Pulsen combine.

Net iD kan konfigureras att antingen låsa användarens dator på operativsystemsnivå eller till att krascha browserprocesser som kör TLS sessioner. Båda dessa metoder är knutna till användarens dator och dess konfiguration. Det är mycket viktigt att användaren förvissar sig om att den egna datorn är korrekt konfigurerad och fungerar på ett tillfredsställande sätt om denna funktion i Net iD avses användas.

7.2 Nedlåsning av datorn

Två olika vägar finns för att låsa klientdatorn vid kortutdrag.

7.2.1 Nedlåsning i operativsystemet

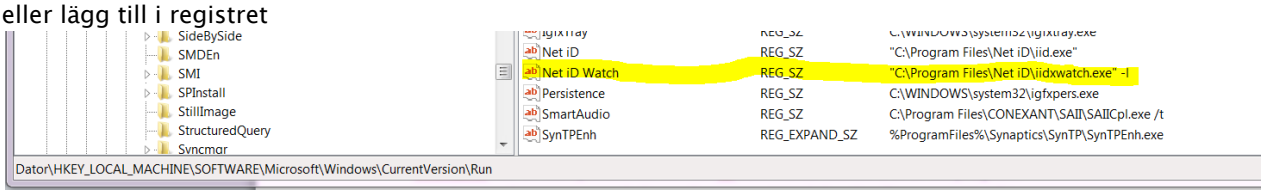
Konfigureras operativsystemet på klienten på sådant sätt att smartkort krävs för inloggning kan även funktion för utloggning eller nedlåsning av klienten sättas upp. Denna typ av lösning måste ses i ett vidare perspektiv då den påverkar hela användarens datormiljö.

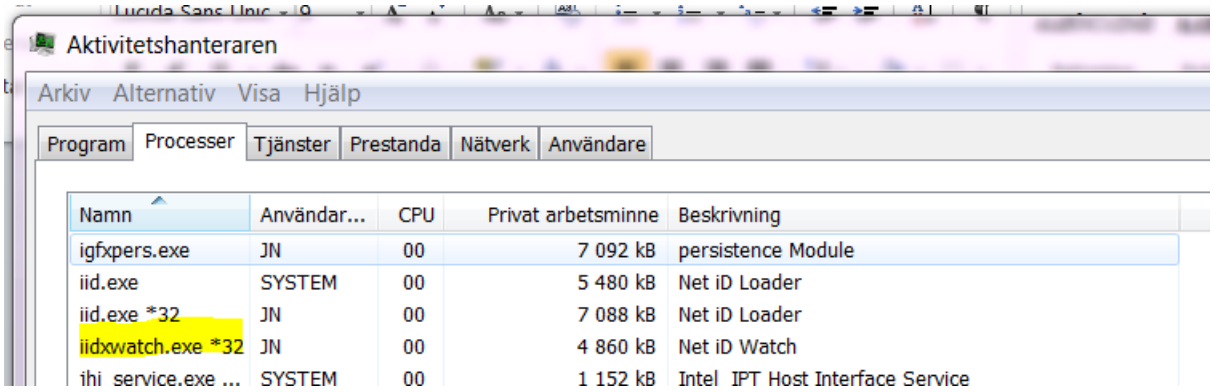
7.2.2 Nedlåsning med hjälp av Watch

Secmaker har en komponent till sin produkt Net iD som kallas Watch. Det är ett program som kan exekveras som en bakgrundsprocess. Watch kan konfigureras att utföra olika saker när den detekterar isättning och urtagning av smarta kort. Watch ingår oftast inte i de grundpaket av Net iD som följer med vid uppsättning av SITHS. För att testa och utvärdera funktionen av Watch kan den startas manuellt eller läggas till i registret. Starta Watch med växeln -l för att få den att låsa klienten vid kortutdrag. Normal konfiguration av Watch sker i Net iDs konfigurationsfil.

c:\program\net id\iidxwatch.exe -l

eller lägg till i registret





Är Watch startad på det här viset kommer den att låsa datorn vid kortutdrag. OBS! smartkortet behövs INTE för att logga in igen. Är datorn konfigurerad för inloggning med användarnamn och lösenord kan användaren logga in med det utan att kortet sitter i kortläsaren. För information om rätt installationspaket och dokumentation om Watch hänvisas till SecMaker.

7.2.3 Browser krasch

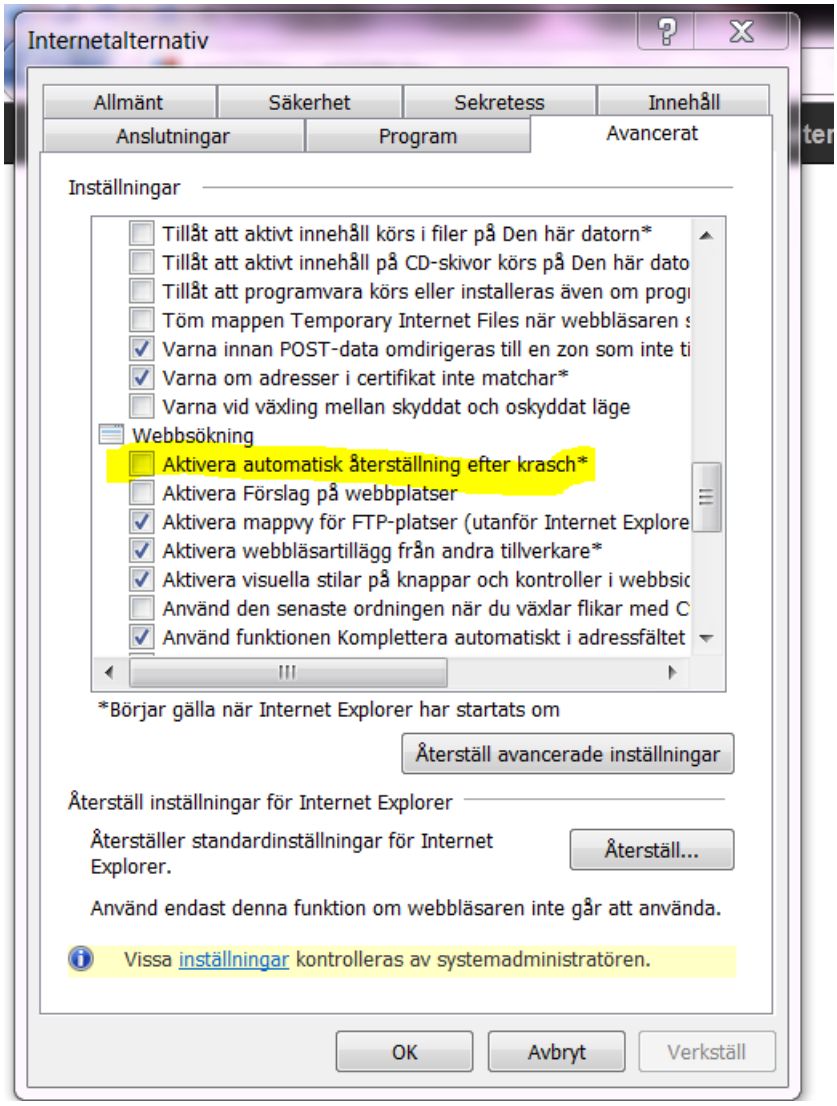
Net iD kan konfigureras att krascha den eller de aktiva browser sessioner som kör TLS sessioner vid det tillfälle smartkort dras ur kortläsaren. För att detta skall fungera måste användarens dator uppfylla ett antal krav. Nedan följer den konfiguration vi funnit fungerande vid test i vår miljö.

- Operativsystem: Microsoft Windows 7 Enterprise 64 sp1
- Net iD: Version 5.6.2.62, SVR1301
- Browser: Internet explorer version 9.0.8112.16421
- Kortläsare: OmniKey 3121
- Drivrutin för kortläsare: HID OMNIKEY3x21 PC/SC Driver version 3.0.2.0

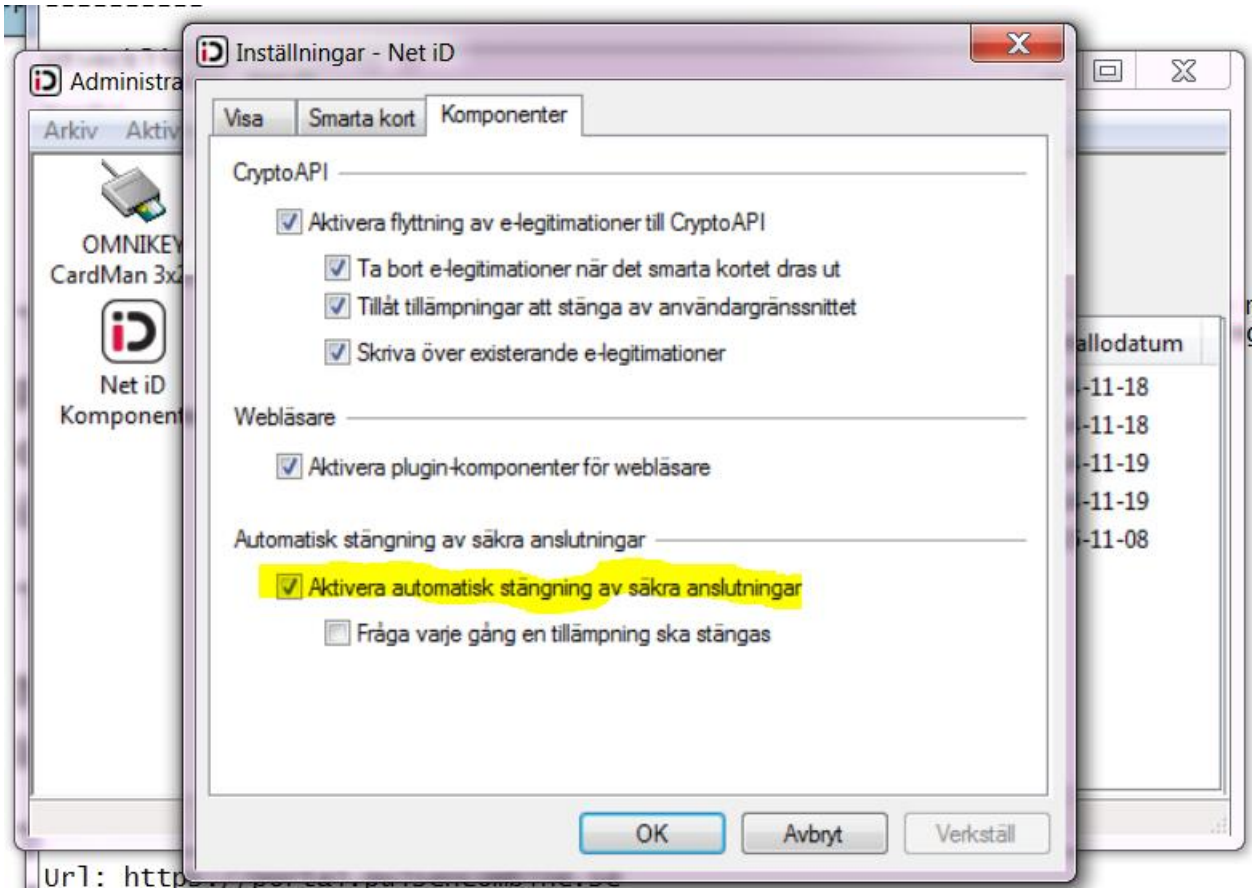
Vidare är det nödvändigt att starta Internet Explorer med växeln -nomerge. Detta förhindrar att sessionsinformation kopieras mellan olika sessioner av Internet Explorer. Startas Internet Explorer utan denna växel kan sessionsdata kopieras mellan olika browsersessioner vilket medför att även om den browser som körts för Pulsen combine stängs kan sessionsinformation finnas kvar i andra browsersessioner.

Internet Explorer har från version 8 en funktion för att automatiskt återställa browsern efter en krasch. Denna funktion är defaultmässigt påslagen och måste stängas av. Inställningen för detta finns under Internetalternativ, flik Avancerat, stycke Websökning. Kryssa ur ”Aktivera automatisk återställning efter krasch”.

Lämnas denna ruta ikryssad kommer Internet Explorer att automatiskt återställa sig efter det att NetID kraschat sessionen. Användaren kommer då direkt att vara tillbaka inne i Pulsen combine på samma ställe som vid utdragande av smart kortet.



Den enda CSP (certificate service provider) som godkänns är SecMakers NetID. Ingen annan CSP får finnas installerad på datorn. Annan SCP kan störa NetID och göra att denna inte kan detektera kortutdragning. NetID skall konfigureras att stänga säkra anslutningar. Se bild.



Det är möjligt att andra versioner av programvaror och drivrutiner kan fungera lika bra. Det är dock upp till användaren och dennes IT-organissation att själva konfigurera och utvärdeta att den egna miljön agerar på ett förväntat sätt vid kortutdragning.

För mer information om SecMakers NetID hänvisas till SecMakers hemsida.

Kopia av iid.cfg från ovan nämnda testmaskin återfinns i slutet av detta dokument

8 Appendix 1

Nedan följer en kopia av konfigurationsfilen för NetID. Betrakta detta som ett exempel på hur konfigurationen kan se ut. Förändring av NetID-paket för produktionsmiljö skall ske i samråd med tillverkaren SecMaker AB.

IID.CFG

```
[Admin Utility]
CheckCaExpire=
CheckCardExpire=30,2.5.4.3=SITHS CA v3;30,2.5.4.3=SITHS CA v5
CheckSoftExpire=0
EnableWinlogon=1
ExplorerMenu=0
InstallPlugins=1
StartMenu=0
TaskbarIcon=1
TaskbarMenuMode=135
UseService=0

[CardBitmap]
Default=iidxcard-default.bmp,0x00150060#0x0000B3:0x00B00076#0xA0A0A0
SITHS CA v3=iidxcard-siths.bmp,0x00400032
SITHS CA v5=iidxcard-siths.bmp,0x00400032
SITHS CA TEST v3=iidxcard-sithstest.bmp,0x00400032
SITHS CA TEST v4=iidxcard-sithstest.bmp,0x00400032
Telia e-legitimation HW CA v1=iidxcard-teliaeleg.bmp,0x00400032
Telia e-legitimation EU HW CA v1=iidxcard-teliaeleg.bmp,0x00400032
Telia Test e-Leg CA v1=iidxcard-teliatest.bmp,0x00400032
Telia Test e-leg CA v2=iidxcard-teliatest.bmp,0x00400032
Telia Card Identifier CA v1=iidxcard-transport.bmp,0x00400032
Telia Card Identifier CA v2=iidxcard-transport.bmp,0x00400032

[Compress]
UncompressOnly=0

[CSP]
AcceptBothKeySet=0
```

AcceptIssuers=
AllowedDuplicateUsage=
CheckRemovalForCSP=Microsoft Base Smart Card Crypto Provider
DeleteAtNewKeySet=0
DenyIssuers=CN=Nordea CA for Smartcard users 10
DisableInsert=0
DisableNonRep=1
DisableRandom=0
DisableSilent=0
Enable=1
EnableFriendName=%subject.2.5.4.3%, %subject.2.5.4.10%
InitChangePin=0
InstallCaCert=0
LoadExternal=0
LoadMyself=0
KeepCertificates=0
KeepRemovedCertificates=0
KeepSessionAlive=0
OverwriteCertificate=1
PublishMachineStore=0
ReplaceCertificate=0
UseCritical=1
VerifyCertificate=0
NamePrefix=Acc Net iD -

[Dialog]
Advanced=1
NoUserInterface=plugin-container.exe

[Dynamic Strings]
Enable=1
SE_1008=Byta säkerhetskod (PIN)
SE_1009=Låsa upp kort (PUK)
SE_1209=Läs in kortet på nytt
SE_1686=Ditt korts SITHS-certifikat (HCC) löper ut om %d dag(ar), vänligen kontakta din kortadministratör för att förnya ditt kort.
SE_2406=Byta säkerhetskod (PIN)
SE_2426=Låsa upp kort (PUK)

SE_2050=Ditt kort har ännu inget HCC. Du kan hämta ditt HCC via SITHS Självadministration om din kortadministratör lagt en beställning för din räkning.
SE_Telia EID IP2c (legitimering)=SITHS-kort (inloggning)
SE_Telia EID IP2c (underskrift)=SITHS-kort (underskrift)
SE_Telia EID IP2i (legitimering)=SITHS-kort (inloggning)
SE_Telia EID IP2i (underskrift)=SITHS-kort (underskrift)
SE_Telia EID IP2s (legitimering)=SITHS-kort (inloggning)
SE_Telia EID IP2s (underskrift)=SITHS-kort (underskrift)
SE_Telia EID IP5a (legitimering)=SITHS-kort (inloggning)
SE_Telia EID IP5a (underskrift)=SITHS-kort (underskrift)

[Encryption]
Format=0

[File Extensions]
Encrypt=p7m
Sign=p7s

[Gina]
DisableChangePassword=0
Enable=0
ErrorOption=0
ExternalGinaDll=msgina.dll
InsertCommand=
HideLockWindow=0
LastLogonDomain=
LastLogonUserName=
LastShutdown=0
LogoFile=iidxlogo.bmp
LogonDomain=
NumLockSet=0
PasswordExpired=0
RemoveCommand=
RequireCard=0
Report=
SelectCertificate=1
ShowScript=0
UseExtraWindow=3
WaitApplications=0

[InitProfiles]
1=

[Install]
Build=SVR1301
Directory=C:\Program Files (x86)\Net iD\
Version=05060262
List=Net iD

[InstallOptions]
MergeOldConfig=0
SpecialBuild=
RemoveOldInstall=1

[Language]
Allowed=
Current=Svenska (SAMSET)

[Links]
Error=
Help=
Mail=smtp:netid@secmaker.com
Support=
Update=

[MiniDriver]
IgnoreLogout=lsass.exe;winlogon.exe;iexplore.exe
RegisterCertificate=
MoveCertificates=0
NamePrefix=Acc Net iD - #

[NetControl]
Applications=iexplore.exe;firefox.exe;safari.exe;chrome.exe;iidxweb.exe
Ask=0
Enable=1

[PCSC]
Enable=1

StateTimeout=0
Unload=1

[Pkcs11]
AlwaysLoginForSSL=0
DetectNewSlots=1
DisableDuplicate=
DisableNonRep=FireFox;Mozilla
EnableExternalMutex=0
LoginTimeout=0
LogoutAtLastSession=
InsertEmptySlots=0
PinMinDigits=0
PinMaxDigits=0
PinReportError=
RandomDisabled=0
ResetTempFiles=0
SinglePin=0
VerifyAlgorithms=0
WaitForSmartCardService=0

[Plugin]
StartService=0

[SingleSignOn]
CSP=0
Disable=
Pkcs11=0
Server=
StartServer=winlogon.exe;lsass.exe;
UseCache=1
UseService=1
UseStored=0

[Smart Card]
PinExpire=0
PinMaxLen=
PinMinLen=
PinType=

Temporary=
TemporaryValidity=30
SecureMessaging=
CreateUpdateCounter=1

[Smart Card Reader]
AllowReaderRemoval=0
Accepted=
CachePath=
CacheValidity=10080
CheckInformation=0
CheckPinPad=0
Denied=Mobile Broadband SIM Card Reader 0;Dell USB Reader 0
Detect=1
KeepLoggedInLocked=0
LockDelay=0
LockTimeout=30
MaxTransfer=255
Mode=1
Poll=333
Protocol=-1
ReloadOnError=1
SingleConnection=1
SystemCacheValidity=10080

[Soft Tokens]
PinExpire=0
PinMaxLen=32
PinMinLen=2
PinType=0
1=

[Watch]
UseService=0

[Watch Insert]
1=

[Watch Remove]

1=

[Trace]
:File=c:\temp\iid.txt
:Admin=c:\temp\iid.txt
:CredentialProvider=c:\temp\iid.txt
:CSP=c:\temp\iid.txt
:Directory=c:\temp\iid.txt
:GINA=c:\temp\iid.txt
:MiniDriver=c:\temp\iid.txt
:Pkcs11=c:\temp\iid.txt
:Plugin=c:\temp\iid.txt
:SSO=c:\temp\iid.txt
:Watch=c:\temp\iid.txt
:Web=c:\temp\iid.txt

[License]
Name=SITHS OEM Software
Company=Inera AB
Value=NC9V-Ez8E-fLon-Va0q-aem8-yFh2

[Custom Links]
SITHS Admin - Via Sjunet=https://ccat.trust.telia.com/ccat
SITHS Självadministration - Via Sjunet=https://ccu.trust.telia.com/ccu
SITHS=http://www.siths.se

[AllowedServers]
https://service.secmaker.com=1
https://netid.trust.telia.com=1
https://cve.trust.telia.com=1

[Credential Provider]
Title=%subject.2.5.4.3%
SubTitle=%subject.2.5.4.10%
TextAbove=%subject.2.5.4.12%
TextBelow=%pinattempts%
Image=BMP(%subject.2.5.4.10%);BMP(%issuer.2.5.4.3%);BMP(NoMatch)
BMP(Landstinget Blekinge)=iidxltblekinge.bmp
BMP(Landstinget Dalarna)=iidxltdalarna.bmp

BMP(Landstinget Gävleborg)=iidxltgavleborg.bmp
BMP(Landstinget Halland)=iidxregionhalland.bmp
BMP(Region Halland)=iidxregionhalland.bmp
BMP(Jämtlands läns landsting)=iidxjll.bmp
BMP(Landstinget i Jönköping)=iidxltjonkoping.bmp
BMP(Landstinget i Kalmar Län)=iidxltkalmar.bmp
BMP(Landstinget Kronoberg)=iidxkronoberg.bmp
BMP(Norrbottens läns landsting)=iidxnll.bmp
BMP(Region Skåne)=iidxregionskane.bmp
BMP(Stockholms Läns Landsting)=iidxsll.bmp
BMP(Landstinget Sörmland)=iidxsormland.bmp
BMP(Landstinget i Uppsala Län)=iidxlul.bmp
BMP(Landstinget i Värmland)=iidxltvarmland.bmp
BMP(Landstinget Västernorrland)=iidxltvasternorrland.bmp
BMP(Landstinget Västmanland)=iidxltvastmanland.bmp
BMP(Västra Götalandsregionen)=iidxvgr.bmp
BMP(Örebro läns landsting)=iidxorebrolt.bmp
BMP(Landstinget i Östergötland)=iidxltostergotland.bmp
BMP(Västerbottens läns landsting)=iidxvasterbotten.bmp
BMP(Carelink AB)=iidxinera.bmp
BMP(Inera AB)=iidxinera.bmp
BMP(SecMaker CA v2)=iidxsecmaker.bmp
BMP(SecMaker CA v3)=iidxsecmaker.bmp
BMP(NoMatch)=iidxnomatch.bmp
BMP(Default)=iidxempty.bmp
CheckDuplicates=0

[Certificate Provider]
Title=%subject.2.5.4.3%
SubTitle=%subject.2.5.4.5%
TextAbove=%subject.2.5.4.10%
TextBelow=Issuer: %issuer.2.5.4.3%
SE_TextBelow=Utfärdare: %issuer.2.5.4.3%
Image=BMP(%subject.2.5.4.10%);BMP(%issuer.2.5.4.3%);BMP(NoMatch)
BMP(Landstinget Blekinge)=iidxltblekinge.bmp
BMP(Landstinget Dalarna)=iidxltdalarna.bmp
BMP(Landstinget Gävleborg)=iidxltgavleborg.bmp
BMP(Landstinget Halland)=iidxregionhalland.bmp
BMP(Region Halland)=iidxregionhalland.bmp

BMP(Jämtlands läns landsting)=iidxjll.bmp
BMP(Landstinget i Jönköping)=iidxltjonkoping.bmp
BMP(Landstinget i Kalmar Län)=iidxltkalmar.bmp
BMP(Landstinget Kronoberg)=iidxkronoberg.bmp
BMP(Norrbottens läns landsting)=iidxnll.bmp
BMP(Region Skåne)=iidxregionskane.bmp
BMP(Stockholms Läns Landsting)=iidxsll.bmp
BMP(Landstinget Sörmland)=iidxsormland.bmp
BMP(Landstinget i Uppsala Län)=iidxlul.bmp
BMP(Landstinget i Värmland)=iidxltvarmland.bmp
BMP(Landstinget Västernorrland)=iidxltvasternorrland.bmp
BMP(Landstinget Västmanland)=iidxltvastmanland.bmp
BMP(Västra Götalandsregionen)=iidxvgr.bmp
BMP(Örebro läns landsting)=iidxorebrolt.bmp
BMP(Landstinget i Östergötland)=iidxltostergotland.bmp
BMP(Västerbottens läns landsting)=iidxvasterbotten.bmp
BMP(Carelink AB)=iidxinera.bmp
BMP(Inera AB)=iidxinera.bmp
BMP(SITHS CA v3)=iidxsiths.bmp
BMP(SITHS CA v5)=iidxsiths.bmp
BMP(SITHS CA TEST v3)=iidxsithstest.bmp
BMP(SITHS CA TEST v4)=iidxsithstest.bmp
BMP(SecMaker CA v2)=iidxsecmaker.bmp
BMP(SecMaker CA v3)=iidxsecmaker.bmp
BMP(Telia e-legitimation HW CA v1)=iidxteliaeleg.bmp
BMP(Telia e-legitimation EU HW CA v1)=iidxteliaeleg.bmp
BMP(Telia Card Identifier CA v1)=iidxteliatransport.bmp
BMP(Telia Card Identifier CA v2)=iidxteliatransport.bmp
BMP(NoMatch)=iidxnomatch.bmp

[Unlock Provider]
ChallengeResponse=0
Timeout=180
Title=%subject.2.5.4.3%
SubTitle=%subject.2.5.4.10%
TextAbove=%subject.2.5.4.12%
TextBelow=%cardlabel%
Image=BMP(Default)
BMP(Default)=iidxlocked.bmp

[Components]
1=EC0939CC3DA8AD02;iid.dll
2=0CDE4990018FD3C7;iidcsp.dll
3=B0A9658A4E4E1770;iidp11.dll
4=5FD48CBCB2290462;iidplg.dll
5=5E90542464240994;iidxmifare.dll
6=AEE268AA5329316A;iidxsso.dll
7=2E4536CED972EF72;iidxcp.dll
8=064C5382DD3414AC;iid.cfg