PLUSFTP

SÄKER FILÖVERFÖRING FÖR SVENSK HÄLSO- OCH SJUKVÅRD

Systembeskrivning

Programversion 1.0

Dokumentversion 1.0, (2011-05-31)

1. Allmän beskrivning 3
1.1. Bakgrund 3
1.2. Grundläggande koncept 3
2. Användarhandledning 5
2.1. PLUSFTP_WIN (Window applikation för manuell överföring) 5
2.2. PLUSFTP_CMD (Kommandoradsprogram) 7
2.3. PLUSFTP_SVC (Windows service) 8
3. Detaljerad beskrivning av vissa funktioner 9
3.1. Arkivering 9
3.2. Mottagningskvitto 9
3.3. Kopiering 9
4. Installation av klient 10
4.1. Förberedelse 10
4.2. Allmänt 10
4.3. Specifikt för PLUSFTP_SVC (Windows service) 11
5. Installation av server 12
5.1. Förberedelser 12
5.2. Packa upp komponenterna 12
5.3. Installera funktionscertifikat för HSA-åtkomst 12
5.4. Lägg upp tjänsten PLUSFTP_WS i IIS 12
5.5. Konfigurera Plus.Config 14
5.6. Konfigurera tillåtna användarcert 14
5.7. Användaregenskaper från fil 14
6. Konfiguration (både klient och server) 16
6.1. Händelselog (ELOG) 16
6.2. Egenskaper 16
6.3. dotNet konfigurationsfil 16
6.4. Konfigurationsfil (plus.config) 16
6.5. Lista med egenskaper 17
6.6. Sökschema för plus.config 20
6.7. Sökväg efter klientcertifikat 21
7. Tips vid installation 22
7.1. Installation av klientcertifikat 22
7.2. Kända svårigheter 23

1. Allmän beskrivning

1.1. Bakgrund

PLUSFTP är ett programpaket för säker överföring av filer inom svensk hälso- och sjukvård. I likhet med andra programvaror för filöverföring (såsom FTP, SFTP) så är dess grundläggande funktion att flytta filer mellan två maskiner via ett nätverk, en lokal maskin (PLUSFTP-klient) och en fjärrmaskin (PLUSFTP-server).

Till skillnad från andra programvaror utnyttjar PLUSFTP den infrastruktur som finns inom svensk hälso- och sjukvård i form av HSA och SITHS för t.ex. autentisering och behörighetshantering. PLUSFTP är dessutom utformat för att följa arkitekturledningens anvisningar vilket bl.a. innebär att alla överföring mellan vårdgivare skall ske mha webb-service, vara krypterad och kräva säkerställd autentisering med certifikat samt att möjlighet skall finnas att erhålla digitalt signerat kvitto på genomförd överföring.

1.2. Grundläggande koncept

PLUSFTP arbetar med några grundläggande koncept.

Överföring sker normalt mellan en ***arbetskatalog*** (på klienten) och en ***virtuell katalog*** (på servern). Med *virtuell* katalog avses att den modell av servern som klienten har är begränsat till en enda katalog. Den virtuella katalogen har, ur klientens perspektiv, heller ingen koppling till dess fysiska plats i filsystemet.

Flera klienter kan använda samma server, men i sin grundkonfiguration är rättigheterna inställda så att den virtuella katalogen är knuten till användarens vårdgivare (dvs. den vårdgivare som finns i medarbetaruppdraget).

Modellen kan liknas vid ***tårtbitar*** där olika användare från samma vårdgivare (inom samma tårtbit) kan se varandras filer, medan användare från olika vårdgivare inte har möjlighet att se varandras filer.

Syftet med PLUSFTP är följaktligen inte att tillhandahålla ett verktyg för klienter från olika vårdgivare att dela information sinsemellan utan att möjliggöra överföring mellan en eller flera klienter och en server från olika vårdgivare.

PLUSFTP ***ingen kontroll av innehållet*** i de filer som överförs. Såväl XML som andra textbaserade format som rena binärfiler kan överföras. Det är med andra ord de parter som sänder respektive tar emot filerna som måste kontrollera att innehållet är korrekt såväl syntaktiskt som semantiskt.

All överföring initieras av klienten och är (i denna version) enkelriktad, från klient till server. Däremot kan information om innehållet i serverns arbetskatalog (dir) överföras överföras till klienten, likaså kan klienten initiera borttagning av filer på servern.

På klienten finns även en ***arkivkatalog***. Klientprogrammen har funktioner för att filer, och i förekommande fall kvitton, efter överföring till servern flyttas till den lokala arkivkatalogen för att därigenom strömlinjeforma en återkommande överföringsprocess.

Det finns tre olika sorters klienter för att tillgodose något olika behov.

a) ***PLUSFTP_WIN*** - En fönsterbaserad applikation där användaren manuellt kan överföra och ta bort filer.

b) ***PLUSFTP_CMD*** - Ett kommandoradsbaserat program avsett att aktiveras tidsstyrt eller via scriptfiler.

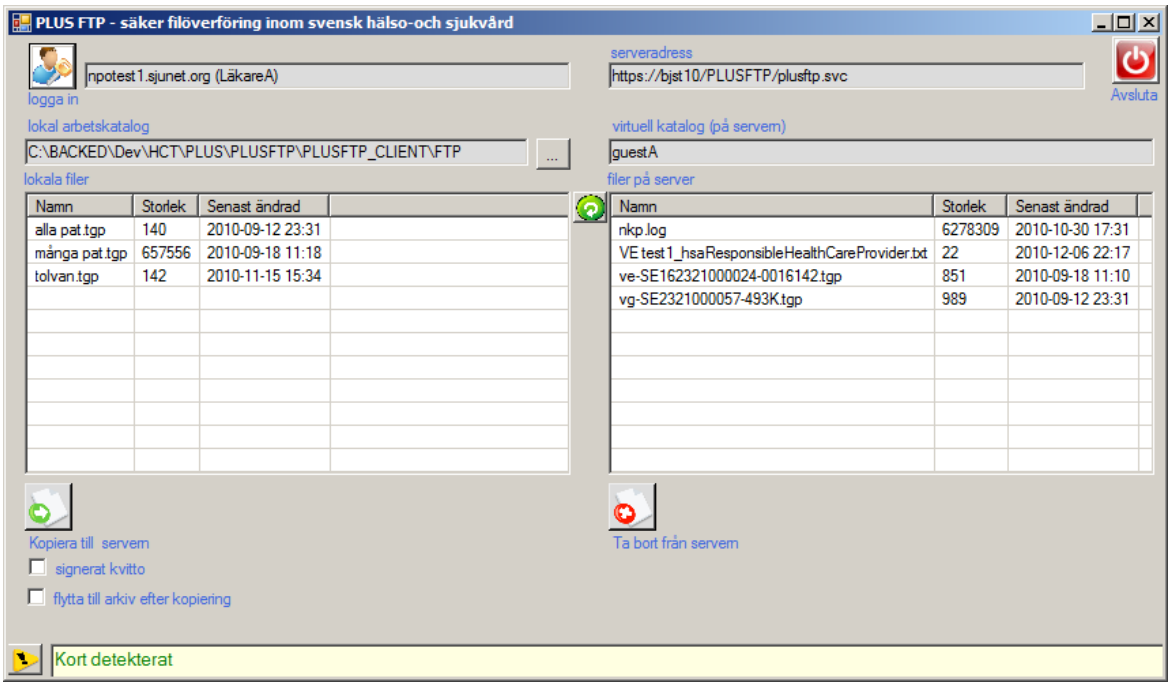
c) ***PLUSFTP_SVC*** - Ett bakgrundsprogram (i form av en Windows service) som kontinuerligt övervakar den lokala arbetskatalogen och överför alla filer som läggs där och därefter flyttar filerna till arkivkatalogen.

Det finns möjlighet för klienten att begära ett ***kvitto*** på genomförd överföring. Detta kvitto utgörs av en digital signatur på PKCS#7-format och är utfärdat av det mottagande systemet. Denna funktion är särskilt viktig vid överföring mellan vårdgivare där ansvarsgränsen utgörs av mottagningsfunktionen, dvs. av PLUSFTP-servern.

All användning kräver att användaren (manuell eller maskinell) **autentiseras**. För manuella användare av *PLUSFTP_WIN* innebär det att de loggar med sitt SITHS-kort, och får sina rättigheter via sitt medarbetaruppdrag (som definieras i HSA). För maskinella användare av *PLUSFTP_CMD* och *PLUSFTP_SVC* innebär det att ett tjänstecertifikat på den lokala maskinen används.

2. Användarhandledning

2.1. PLUSFTP_WIN (Window applikation för manuell överföring)



I fönstrets övre del framgår vem som för tillfället är inloggad, sökvägen till den lokala arbetskatalogen, url till serven samt namnet på den virtuella katalogen.

Programmets mittsektion visar filerna på den lokala arbetskatalogen (i listan till vänster) och filerna på den virtuella katalogen (till höger).

I nedre delen finns knappar för programmet huvudfunktioner.

Längst ner finns en statusrad som visar resultatet av senaste aktiviteten.

2.1.1. Kopiera filer till den virtuella katalogen på servern

1. Markera en eller flera lokala filer. Flera filer kan markeras genom shift-klick (intervall) eller ctrl-klick (enstaka).
2. Markera eventuellt om signerat kvitto ska skickas tillbaka från servern eller om den lokala filen ska flyttas till arkivet efter kopiering till servern.
3. Tryck på knappen *Kopiera till servern.*
4. Filerna kopieras nu.

2.1.2. Ta bort filer från den virtuella katalogen

1. Markera en eller flera filer i den virtuella katalogen (till höger).
2. Tryck på knappen *Ta bort från servern.*
3. Filerna tas nu bort.

2.1.3. Ladda om de båda listorna

1. Tryck på omladdningsknappen mellan listorna 
2. Listorna laddas om.

2.1.4. Logga in och Logga ut

1. Programmet känner automatiskt av när det finns ett tillgängligt certifikat för inloggning och visar då upp dialogrutan för certifikatval. Normalt sker det i samband med att kortet sätts in i kortläsaren, men i de fall det finns mjuka certifikat installerade så kommer dessa att detekteras redan innan kortet satts i läsaren och certifikatvalsdialogen visas. Välj i så fall avbryt, stoppa in kortet och vänta på att certifikatvalsdialogen visas på nytt.

2. Efter val av certifikat så visas dialogen för val av medarbetaruppdrag.
   Markera ett medarbetaruppdrag och tryck OK (eller dubbelklicka direkt på medarbetaruppdraget)

3. Inloggning klar.

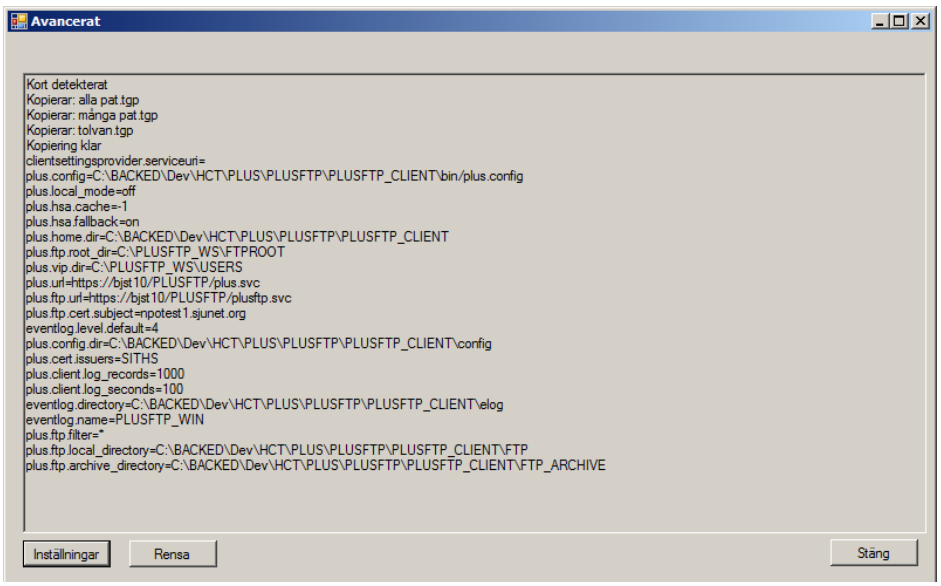
Avslut sessionen kan ske antingen explicit genom att trycka på *Logga in* på nytt och välja avbryt eller genom att avsluta programmet eller genom att dra ut kortet ur läsaren.

OBS – Det enda som utgör en riktig utloggning är när kortet tas ur läsaren eftersom det normalt inte erfordras någon ny pin-kod så länge kortet sitter kvar i läsaren (vilket är en NetId-konfigurering).

2.1.5. Se detaljer

För att se mer detaljer i form av historik från den aktuella sessionen, eventuella felutskrifter i detalj eller aktuell konfiguration.

1. Tryck på knappen  längst nere till vänster.
2. Ett nytt fönster öppnas.
3. Tryck på knappen *Inställningar* för att visa aktuella inställningar (egenskaper).
4. Tryck på Rensa om du vill rensa texten i fönstret.



2.2. PLUSFTP_CMD (Kommandoradsprogram)

Programmet startas från kommandoraden eller via script eller andra program.

Giltiga kommandon

`help`	Visar hjälptext
`config`	Visar aktuell konfiguration, dvs aktuella egenskaper
`send <filnamn> [-r] [-a]`	Överför angiven fil. Filnamnet skall anges med fullständig sökväg.
`sendall [-r] [-a]`	Överför alla filer i den lokala arbetskatalogen
`dir [filter]`	Visa filer i den virtuella katalogen (på servern)
`delete <filnamn>`	Ta bort angiven fil från den virtuella katalogen (på servern).

Växlar

`-r`	Begär signerat kvitto
`-a`	Flytta till arkiv efter överföring

2.3. PLUSFTP_SVC (Windows service)

Programmet är avsett att exekvera som Windows service och saknar därmed användargränssnitt.

Programmet kan även aktiveras från kommandoraden vilket kan vara bra för teständamål.

Start av programmet

`C:\>PLUSFTP_SVC run`	Startar programmet i kommandoradsläge vilket innebär att det har samma funktion som vid exekvering som Windows service, med den skillnaden att det avslutas som ett standard windowsprogram.

3. Detaljerad beskrivning av vissa funktioner

3.1. Arkivering

Vid arkivering flyttas filen till arkivkatalogen efter överföring. Detta sker oberoende av varifrån filen hämtas. (Via PLUSFTP_CMD anges ju filer med absolut sökväg).

Om en fil med samma namn redan finns i arkivet kommer den aktuella filen döpas om så att den innehåller aktuell tid på formatet YYYYMMDD-hhmmss.

Exempel:
`myfile.txt` får namnet `myfile(20101221-142036).txt`

3.2. Mottagningskvitto

Vid begäran om mottagningskvitto (kryssrutan *signerat kvitto* i plusftp_win, växeln -r i plusftp_cmd) skapas en digital signatur på pkcs#7-format av servern. Signaturen är s.k. *detached*, dvs den signaturen omsluter inte det signerade dokumentet utan är frikopplad från det kopierade dokumentet. Signaturen är därför alltid ca 1,5 kB stort oberoende av dokumentets storlek.

Signaturen innehåller även certifikatet som användes vid signering (men inte utfördarcertifikaten), signeringstid (serverns tid), och filnamnet (utan sökväg) på den fil som kopierats. Filnamnet finns med som information och är därför ett osignerat attribut.

När kvittot ta emot görs en kontroll av att den kryptografiskt stämmer med den fil som skickats iväg. I och med detta garanteras också att filen inte förvanskats vid överföringen.

Kvittot sparas lokalt i samma katalog som den aktuella filen och får samma filnamn förlängt med filslut ”.p7s”. Det innebär att vid arkivering så kommer även kvittot att sparas i arkivkatalogen.

3.3. Kopiering

Filer behåller sitt filnamn och sin tidsstämpel (senast sparad) vid kopiering till den virtuella katalogen. Om en fil med samma namn redan finns så kommer den att ersättas med den nya filen.

4. Installation av klient

4.1. Förberedelse

4.1.1. dotNet - framework

PLUSFTP baseras på Microsofts dotNet-plattform som ingår som en del i Windows operativsystem. PLUSFTP använder version *4.0 full*, och eventuellt kan den aktuella versionen på arbetsstationen behöva uppgraderas.

Enklaste sättet att ta reda på vilken version som redan är installerad är att köra programmet *dotnet.exe* som kan laddas hem gratis via http://www.asoft.be/downloads/netver2007.zip

Uppgradering av dotNet görs via Microsofts hemsida (kostnadsfritt)

Direktlänk:
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=9cfb2d51-5ff4-4491-b0e5-b386f32c0992&displaylang=en

4.1.2. Kort, kortläsare

PLUSFTP använder inloggning med SITHS-kort. Användaren måste ha ett SITHS-kort samt kortläsare och nödvändig säkerhetsklient (NetId) installerad.

4.1.3. PLUSFTP Server

Det måste finnas en PLUSFTP-server som användarna har tillgång till. För att få åtkomst till servern krävs att användaren har ett medarbetaruppdrag i HSA-katalogen med de rättigheter som erfordras för den aktuella PLUSFTP-servern.

4.1.4. Funktionscertifikat

För användning av *PLUSFTP_CMD* och *PLUSFTP_SVC,* som innebär att inloggning sker utan att någon manuell användare medverkar aktivt, måste ett tjänstecertifikat finnas installerat på den lokala maskinen.

4.2. Allmänt

4.2.1. Packa upp zip-filen

Installationen är packad i en zip-fil. Packa upp zip-filen till valfri plats på arbetsstationen. Det kan vara lämpligt att lägga leveransens huvudkatalog (PLUSFTP_CLIENT) direkt under C:\ eller under C:\program. Alla tre klientprogrammen ligger i samma katalog (/bin) och packas upp samtidigt.

4.2.2. Gemensam konfiguration.

Nödvändig konfigurering görs i filen filen Plus.Config. Det flesta egenskaper är förkonfigurerade eller har relevanta default-värden, men följande egenskaper måste anges.

- plus.url
- plus.ftp.cert.subject
- plus.ftp.url

Se detaljerad beskrivning nedan av konfigurerbara egenskaper.

4.3. Specifikt för PLUSFTP_SVC (Windows service)

Servicen installeras och avinstalleras genom att programmet plusftp_svc startas via ett kommandofönster med argumntet --install respektive --uninstall (notera dubbla minustecken).

Exempel:

```
c:\plusftp_client\bin>plusftp_svc –install
c:\plusftp_client\bin>plusftp_svc –uninstall
```

PLUSFTP_SVC är konfigurerad för att starta manuellt. Om automatisk start önskas måste detta konfigureras via Windows tjänstekonfiguration.

För PLUSFTP_SVC måste konfigurationsfilen användas för att ange om mottagningskvitto ska begäras vid sändning. (Egenskapen *plus.ftp.receipt*).

5. Installation av server

5.1. Förberedelser

För att kunna installera och starta PLUSFTP_WS krävs att följande förutsättningar av mer generell karaktär är uppfyllda.

1. En maskin med Windows operativsystem finns tillgänglig.
2. dotNet runtime 4.0 är installerat (se 4.1.1)
3. IIS
4. Åtkomst av Sjunet
5. Fysisk åtkomst till HSA-katalogens WS-tjänster
6. Installerat maskincertifikat (kan beställas från SITHS) för inkommande anrop. Certifikatnamnet måste matcha maskinens namn för att användarna ska slippa varningsmeddelanden.
7. Funktionscertifikat för åtkomst av HSA-katalogens WS-tjänster (kan med fördel vara samma som ovanstående)
8. Rättigheter för funktionscertifikatet att komma åt WS-tjänster i HSA (GetMiuForPerson).. (Via HSA-förvaltningen)
9. Ett användarkonto med systemrättigheter för installation.

5.2. Packa upp komponenterna

1. Packa upp zipfilen till valfri katalog i filsystemet.

5.3. Installera funktionscertifikat för HSA-åtkomst

Installera funktionscertifikatet för HSA-åtkomst i ”Lokal dator” - ”Personliga” (*Local Machine – Personal/My*).
T.ex. genom användning av MMC. (Se kap 7.1).

5.4. Lägg upp tjänsten PLUSFTP_WS i IIS

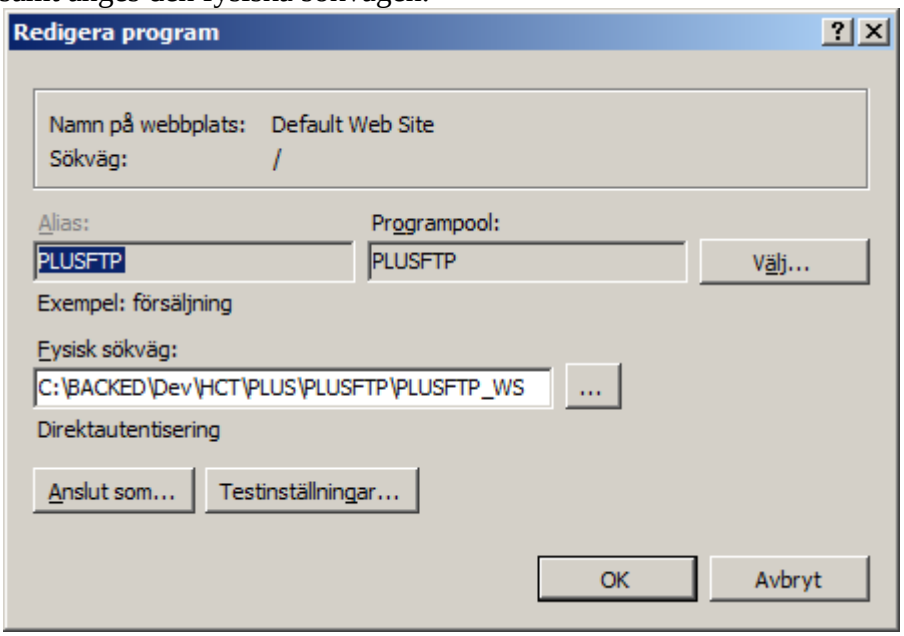
Handhavande av IIS beskrivs endast översiktlig i detta dokument. Istället hänvisas till tillverkarens (Microsoft) dokumentation.

1. Skapa en programpool
   (Programpooler->Avancerade inställningar -> Lägg till programpool)
   Brukligt är att ha samma namn på programpoolen som på programmet, i detta fall PLUSFTP_WS.

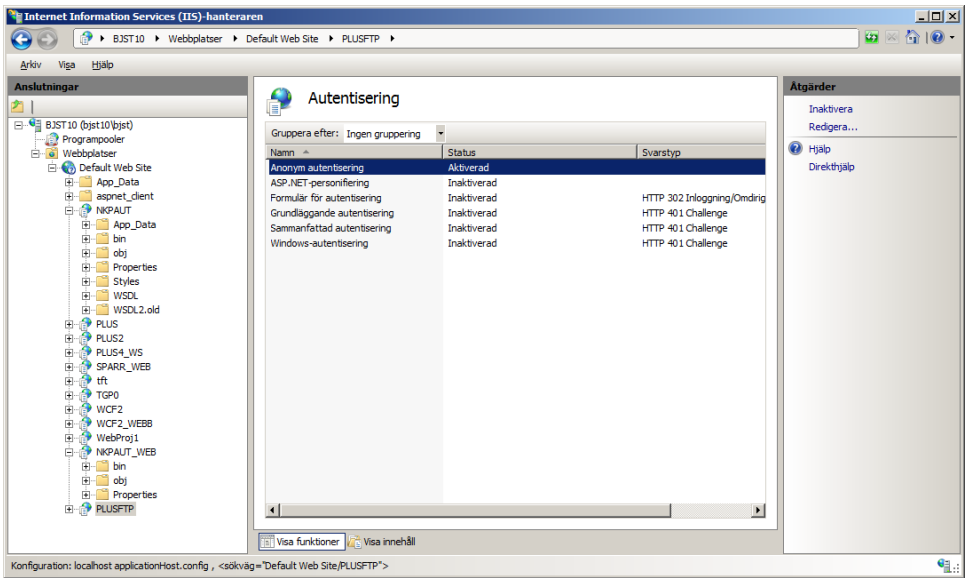
2. Knyt programpoolen till en användare med systemrättigheter (för att komma åt cert i Lokal dator) samt rättighet att skriva och läsa på katalogerna NKPAUT och PLUSHOME.
   (Programpooler->Avancerade inställningar -> identitet)
   LocalSystem är avsett för detta.

3. Lägg till tjänsten PLUSFTP_WS
   Default Web Site->Lägg till program

4. Välj programpoolen PLUSFTP_WS och ge programmet ett namn (t.ex. PLUSFTP_WS) samt anges den fysiska sökvägen.

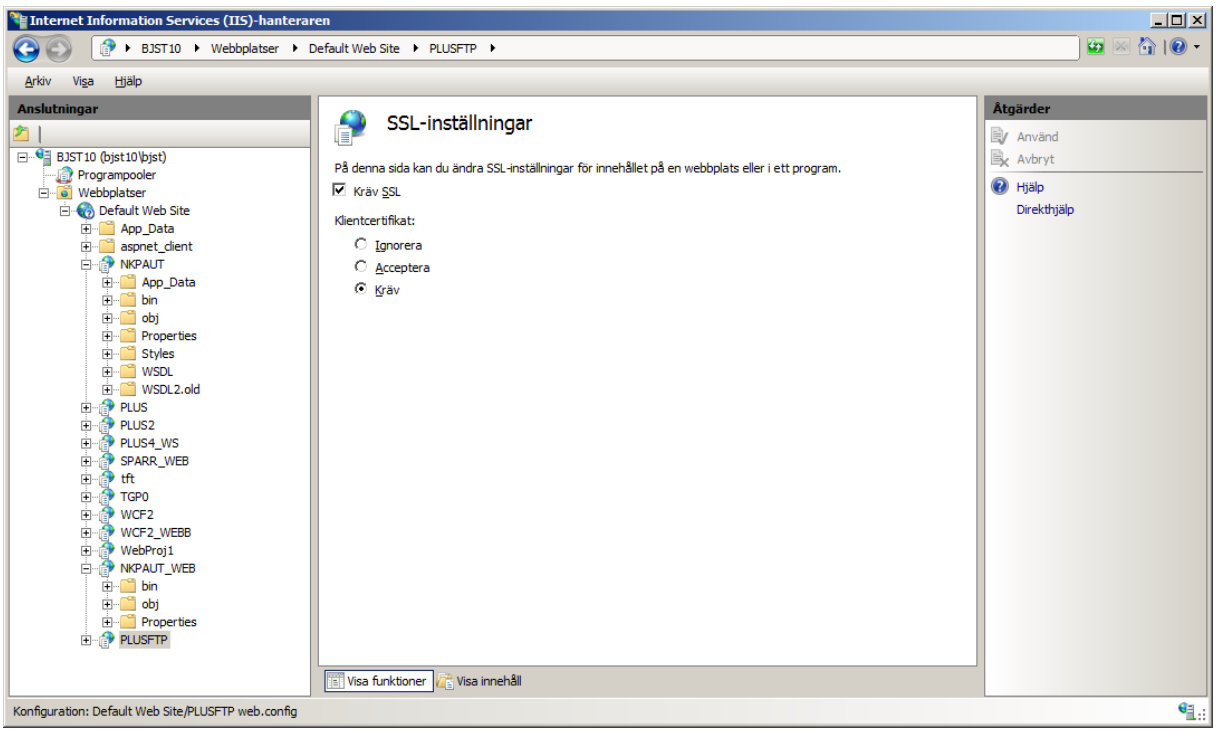


5. Aktivera anonym autentisering
(Autentisering -> Anonym autentisering -> Aktivera)



6. Aktivera dubbelriktad autentisering med certifikat.
Kräv SSL – Kräv
Detta ska matcha inställningen för bindingConfiguration `i Web.config`

```
 <security mode="Transport">
  <transport clientCredentialType="Certificate" />
</security>
```



5.5. Konfigurera Plus.Config

Se kap 6.4

5.6. Konfigurera tillåtna användarcert

Se till att de publika certifikaten för utfärdare till de kort som skall vara tillåtna att logga in med finn i certifikatkatalogen ”betrodda rotcertifikatutfärdare”. Typiskt är dessa SITHS CA v3, SITHS CA v4 och för test dessutom SITHS CA TEST v3 och SITHS CA TEST v4.

Det är endast certifikat av dessa utfärdare som visas för användaren vid inloggning.

5.7. Användaregenskaper från fil

5.7.1. Kända användare

Om HSA-katalogens WS-tjänster inte är tillgängliga eller det finns användare som ska komma åt tjänsten men som inte finns i HSA så finns möjlighet att definiera dessa användare och deras egenskaper på fil.

I katalogen som pekas ut av plus.vip.dir (normalt [plus.home.dir]\users) så kan användarfiler skapas. Dessa har filnamn på formatet : <hsa-id>#<unik del>.txt

Samma användare kan ha flera filer, en för varje medarbetaruppdrag.

Den medföljande filen (template.txt) tjänar som förlaga för att lägga upp nya filer.

5.7.2. Tillfälliga användare från fil

Om det finns en (eller flera) filer med text *guest* istället för <hsa-id> så kommer programmet automatiskt använda denna som förlaga för användare som inte redan finns definierade eller finns i HSA-katalogen.

För var och en av dessa användare skapas därefter egna filer på med hsa-id i namnet.

6. Konfiguration (både klient och server)

6.1. Händelselog (ELOG)

Det är förvånansvärt mycket som kan gå fel vid arbete med kommunikation och säkerhetskonfiguration. Detta innebär en extra svårighet för bakgrundsprogram eller program med ett begränsat användargränssnitt. PLUSFTP är utformat för att i möjligaste mån fånga de felsituationer som kan uppstå och underlätta felsökning genom att logga händelser i en händelselogg (event log).

Händelseloggen utgörs av textfiler med programnamn och tidsstämpel i filnamnet. Filerna lagra på en filkatalog som pekas ut vid konfigureringen.

Alla som kommit så här långt i dokumentationen kommer också ha behov av att titta i händelseloggen. Ägna någon minut åt att ställa in relevanta egenskaper och lokalisera händelseloggen i filsystemet.

6.2. Egenskaper

Programmen styrs av en rad konfigurerbara egenskaper (se tabellen nedan).

Värdet på dessa egenskaper sätts enligt följande sökschema

1. Som argument på kommandoraden på formatet *egenskap=värde*

2. Via dotNet:s konfigurationsfil som applikationsegenskaper (key)
   Exempel:
   ```
   <configuration>
     <appSettings>
       <add key="plus.config" value="my_plus.config" />
       ...
   ```

3. Via filen plus.config.

Egenskaperna läses endast in vid programstart. För bakgrundsprogram (PLUSFTP_SVC och PLUSFTP_WS) innebär det att dessa måste startas om för att få effekt.

6.3. dotNet konfigurationsfil

dotNet använder konfigurationsfiler på ett fördefinierat XML-format som standard.

För webbservice-program används filen *web.config* på den katalog som pekas ut i IIS.

För lokala exekverbara program används en fil i samma katalog som det exekverbara programmet och med samma namn förlängt med .config.

Exempel: *plusftp_win.exe.config*.

6.4. Konfigurationsfil (plus.config)

Filen plus.config är den som normalt används för merparten av de egenskaper som skall definieras.

Den innehåller rader på formatet

```
egenskap = värde
```

I övrigt gäller följande syntaxregler:

- En egenskap per rad
- ! (utropstecken) kan användas i början av raden som kommentarstecken
- Tomma rader ignoreras
- Såväl värde som egenskap kan omges av godtyckligt antal blanktecken
- Blanktecken inne i värdet kan förekomma
- Om samma egenskap förekommer flera gånger kommer den första att användas
- Logiskt värde för sant kan anges som något av *t, y, 1, s, true, yes, sant, on* eller tomt. Övriga värden betraktas som falskt. Värdet är oberoende av versaler/gemener.

6.5. Lista med egenskaper

[egenskap] = värdet av angiven egenskap

*** = egenskapen sakar default-värde (måste fyllas i om funktionen ska kunna användas)

Kolumn x = anger om egenskapen är relevant på klientsidan (k) eller serversidan (s) eller båda (ks)

Egenskap	Beskrivning	default	x
PLUSFTP KLIENT	Specifika egenskaper för PLUSFTP		
plus.ftp. archive_directory	Lokal arkivkatalog, dvs dit filer som har överförts flyttas om arkivering begärs i samband med överföring.	[plus.home.dir]\ ftp_archive	k
plus.ftp. archive_directory	Lokal arkivkatalog, dvs dit filer som har överförts flyttas om arkivering begärs i samband med överföring.	[plus.home.dir]\ftp _archive	k
plus.ftp. cert.subject	Namn (subject) på det certikat som används för PLUSFTP:s maskinella användare vid autentisering och anslutning till PLUSFTP-tjänsten. Not. För manuella användare används användarens certifikat (SITHS-kort) istället.	***	k
plus.ftp. filter	Filfilter som begränsar de filer som är synliga för användaren (både på den lokala arbetskatalogen och på den virtuella katalogen på servern). Exempel: `plus.ftp.filter = *.tgp`	alla filer (*)	k

plus.ftp. local_directory	Lokal arbetskatalog, dvs där filer som skall överföras till servern ligger.	[plus.home.dir]\ftp	k
plus.ftp. receipt	Anger att kvitta ska begäras vid sändning. Endast tillämpligt i PLUSFTP_SVC där detta inte kan styras på annat sätt.	off	k
plus.ftp. url	URL till PLUSFTP-tjänsten	***	k
PLUSFTP SERVER			
plus.ftp. root_dir	Root-katalog för virtuella kataloger	[plus.home.dir]\ ftp_root	s
plus.ftp. signcert.subject	Namn (subject) på det certikat som ska användas för signerade svar.	[plus.ftp. cert.subject]	s
PLUS KLIENT	Generella inställningar för PLUS säkerhetstjänst		
eventlog. directory	Filkatalog för händelselog (Event log)	[plus.home.dir]\ elog	ks
eventlog. name	Programnamn vid användning av händelselog. Programnamnet ingår som en del i det filnamn som skapas. Om flera program använder samma katalog kan det vara praktiskt att mha filnamnet se vilket program som skapar vilket fil.	programmets startmodul	ks

eventlog.
level
eventlog.
level.<module>
	Nivå på de händelser som ska loggas.
	1=error, 2=warning, 3=info, 4=verbose.
	Alla händelser med samma eller lägre nivå än angiven loggas.
	Om ingen modul anges (eller anges som ”default”) gäller samma nivå på alla händelser. Det dock går att specificeras en eller flera moduler med annan nivå.
	I nedanstående exempel är utökad loggning påslagen för modulen HSAMGR.
	`eventlog.level.default = 2`
	`eventlog.level.HSAMGR = 4`
	…
		1	ks

plus. cert.issuers	Kommaseparerad lista med godkända utfärdarnamn av de autentiseringscertifikat som ska visas för en manuell användare vid inloggning. Utfärdarnamnet behöver inte matchas exakt. Det räcker att texten i angivet	SITHS	k

	utfärdarnamn ingår i certifikatets utfärdarnamn.		
plus. client.cert.subject	Namn (subject) på det certikat som används vid kommunikation med PLUS-tjänsten.	***	k
plus. client.log_records	Antalet loggposter som samlas ihop i en bunt innan överföring sker till loggtjänsten. Överföring initieras när maxgränsen är nådd för antal poster eller tid.	1000	k
plus. client.log_seconds	Max tid innan överföring av en bunt sker till loggtjänsten. Överföring initieras när maxgränsen är nådd för antal poster eller tid.	100	k
plus. config	Anger, efter inläsning av plus.config, filnamnet på de inlästa filerna i den ordning de lästs in. Kan ej definieras i plus.config.	-	ks
plus. config.dir	Katalog för ytterligare konfigurationsfiler, bl.a. maskincertifikat på fil.	[plus.home.dir]\ config	ks
plus. home.dir	Hemkatalog för plus. Denna utgör default root-katalog för övriga PLUS-kataloger	***	ks
plus. local_mode	Endast för test on = anslut en lokal PLUS-tjänst (i samma process). off = använd WS-baserad PLUS-tjänst.	off	k
plus. url	URL till PLUS-tjänsten	***	k
PLUS SERVER			
plus. accesscontrol	Aktiverar funktion för åtkomstkontroll på serversidan anropsbar från klienten. (Serverprogram som är hoplänkade med PLUS, tex. PLUSFTP, kan använda funktionen ändå)	off	s
plus. authentication	Aktiverar autentiseringsfunktionen på serversidan.	on	s
plus. block	Aktiverar funktion för spärrar på serversidan. Kräver att databasen aktiveras.	off	s
plus. consent	Aktiverar funktion för samtyckeshantering på serversidan.	off	s

	Kräver att databasen aktiveras.		
plus. db.connectionString	Uppkopplingssträng vid användning av SQL-databas (krävs då loggning, samtycke eller spärr är aktiverat)	***	s
plus. hsa.adress	URL till HSA-katalogens webb-tjänster.	***	s
plus. hsa.cache	Tid (i minuter) för hur länge resultatet av värden som tidigare hämtats från HSA-katalogen ska återanvändas, dvs. läses från den filbaserade cachen. 0 = fråga alltid HSA (avstängd cache) -1 = fråga aldrig HSA	10	s
plus. hsa.cert.subject	Certifikatnamn (subject) på det certifikat som används vid kommunikation med HSA-katalogens webb-tjänster.	***	s
plus. hsa.dir	Katalog för cachelagring av HSA-slagningar	[plus.home.dir]\hsa	s
plus. hsa.fallback	Anger att senast kända värde (från cachen) ska användas om HSA-katalogen är otillgänglig. Om funktionen är avstängd samtidigt som *plus.hsa.cache*=0 så lagras inga värden i cachen.	on	s
plus. log	Aktiverar loggfunktionen på serversidan. Kräver att databasen aktiveras	off	s
plus. log.dir	Arbetskatalog på servern för logfiler (som skickas från klienten)	[plus.home.dir]\log	s
plus. rules.dir	Arbetskatalog på servern för behörighetsregler.	[plus.home.dir]\ rules	s
plus. session.timeout	Livslängd för en inloggningssession för en inaktiv användare (sekunder).	3600	s
plus. test.dir	Endast för test	[plus.home.dir]\test	s
plus. vip.dir	Arbetskatalog på servern för användar-egenskaper på fil.	[plus.home.dir]\ users	s

6.6. Sökschema för plus.config

PLUSFTP letar efter filen plus.config enligt följande sökschema.

1. En fil som pekas ut explicit i dot-NET inbyggda konfigurationsfiler.
   Dessa är web.config för PLUSFTP_WS samt filer med samma grundnamn som motsvarande exekverbar program, med filslut Config (t.ex. PLUSFTP_WIN.exe.config).
2. En fil med namnet *plus.config* i samma katalog som den exekverbara filen, och därefter i alla i alla överliggande kataloger nerifrån och upp. Samtliga filer som hittas på detta sätt genomsöks men bara den första förekomsten av varje egenskap läses in.
3. En fil med namnet *plus.config* i hemkatalogen, dvs. den katalog som anges av egenskapen *plus.home.dir*. Detta förutsätter att hemkatalogen anges i dot-NET inbyggda konfigurationsfiler.
4. En fil som pekas ut genom miljövariabeln *plus.home.dir*
5. En fil med namn *plus.config* på katalogen C:/PLUS

Ett tips är att placera *plus.config* i en katalog en eller ett par nivåer ovanför den exekverbara filen. Detta ger möjlighet att dela konfiguration mellan olika program som kanske inte ligger i samma katalog. Samtidigt kan en *plus.config* med mindre avvikelser läggas längst ner i sökvägen för att åstadkomma speciell konfigurering för en viss exekverbar modul.

6.7. Sökväg efter klientcertifikat

PLUS söker efter maskincertifikat för autentisering enligt följande sökschema.

1 Ett matchat par av filer i katalogen plus.config.dir med filnamn (utan filslut) som anges av den aktuella egenskapen (t.ex. *plus.client.cert.subject*).
Den ena filen utgör certifikataet på p12-format med filändelse .p12 och den andra pin-koden till certifikatet med filändelse .pin.
OBS – denna metod att ange certifikatet bör inte användas i för produktionscertifikat eftersom pin-koden är oskyddad.

2 I certifikatlagret (certificate store) för aktuell användare (CurrentUser) med ämne (subject) som börjar på ämne som anges av egenskapen plus.client.cert.subject och med typ avsett för autentisering (0xA0).
Om flera certifikat matchar så väljs det första.

3 Som ovan men för lokal maskin (LocalMachine)

PLUS söker efter maskincertifikat för signering enligt samma sökschema som ovan, med den skillnaden att sökning sker i första hand efter certifikat med avsedda för signering (0x40) och därefter efter certifikat avsedda för autentisering.

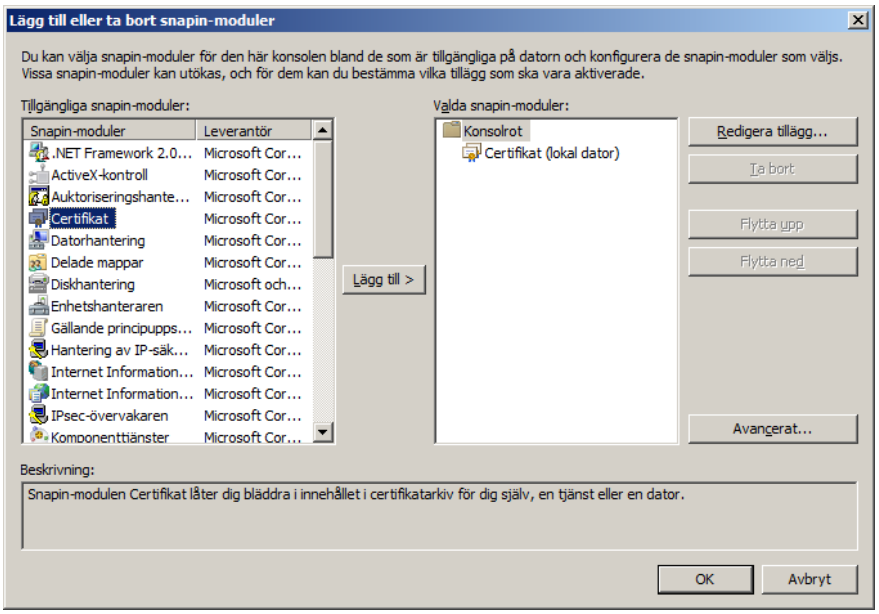
Det kan synas märkligt att signera med certifikat avsedda för autentisering, men för maskiner finns ofta endast ett certifikat och rent tekniskt är det exakt samma process oavsett certifikatets syfte.

7. Tips vid installation

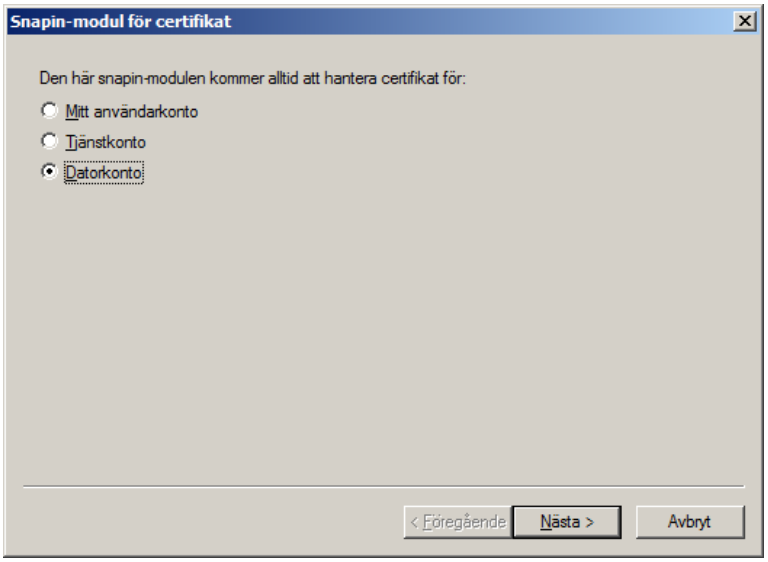
7.1. Installation av klientcertifikat

För installation av tjänstecertifikat används lämpligen programmet **mmc**.

Detta startas från startmenyn eller från (C:\Windows\System32)



Välj Datorkonto om det är Local machine/Lokal dator som ska hanteras



7.1.1. Notera

Notera att det krävs **systemrättigheter** för den process/användare som skall nyttja ett installerat tjänstecertifikat.

7.2. Kända svårigheter

7.2.1. Testkort - SITHS CA Test V4

Normalt ligger utfärdarcertifikatet med på de SITHS-kort som distribueras vilket gör att användaren automatiskt får en fråga första gången om utfärdarcertifakatet skall importeras.

För vissa testkort med utfärdare *SITHS CA Test V4* saknar emellertid utfärdarcertifikatet på kortet. Detta måste då hämtas och importeras manuellt innan kortet kan användas.

Symptomet är att inga certifikat visas i certifikatvalsdialogen.

7.2.2. Java och certifikat

OBS. Java har en egen ”store” för godkända certifikat vilket gör att Javaprogram kräver hantering vid sidan om maskinens egna ”store”.