

# Installationsvägledning Multifråga

1. Installationsvägledning .....	1
1.1. Windows Server 2008R2 med IIS7 .....	2
1.1.1. Att skapa en IIS-sajt (2008R2) .....	2
1.1.2. Att kopiera in distributionen (2008R2).....	3
1.1.3. Att definiera filrättigheter (2008R2).....	3
1.2. Windows Server 2003 med IIS6 .....	4
1.2.1. Att skapa en IIS-sajt (2003) .....	4
1.2.2. Att kopiera in distributionen (2003) .....	5
1.2.3. Att definiera filrättigheter (2003).....	5
1.3. Att installera klient-certifikat för SHS-IWSI (ifall behövs) .....	6
1.4. Att modifiera web.config .....	8
1.5. Loggfiler .....	9
1.6. Felsökningstips .....	10
1.7. Multifråga som ”slav” under verksamhetsapplikation.....	11

## 1. Installationsvägledning

Denna installationsvägledning handlar om installation av själva webbapplikationen i en befintlig ASP.NET-server (främst Windows Server 2003 och 2008R2). Vägledningen används med fördel tillsammans med checkliste-dokumentet *Multifraga\_checklista\_drift\_2010-01-18.doc* (eller senare version) som behandlar hela driftuppsättningen, inte bara webbapplikationen.

Andra varianter än nedan beskrivna är självfallet möjliga, IIS/ASP.NET-kunnig personal kan tänkas utforma andra lösningar baserat på applikationskodens egenskaper och konfigurationsparametrarna. Observera dock att det är ganska snårigt i IIS/ASP.NET att gå ifrån den inloggningskonfiguration som beskrivs nedan.

## 1.1. Windows Server 2008R2 med IIS7

### 1.1.1. Att skapa en IIS-sajt (2008R2)

Kolla att ASP-rollen finns definierad för servern:

- Gå in i Server Manager
- Expandera Roles i vänsterträdet, välj sen Web Server (IIS), gå ner till höger till Role Services, se ifall ASP.NET är installerad.
  - Om icke, klicka Add Role Services, välj ASP.NET och installera.

Fortsätt i Server Manager, i trädet till vänster, expandera IIS, i trädet i mitten, expandera ner till Sites, skapa ny sajt:

- Namn Multifraga
- Välj Classic .NET AppPool (dvs IIS6-emuleringen, inte ”äkta” IIS7 mode)
- Physical path: Skapa *C:\inetpub\wwwroot\Multifraga\_dir* härinne, inte i vanliga Winexplorer.
- Välj http ifall säkring sker t ex med Citrix, annars https och ange ett cert enligt kommunens normala rutiner för interna SSL-sajter.

Välj sajten i trädet och:

- Dubbelklicka Default Document och addera *default.aspx* överst till listan om det inte redan finns.
- Dubbelklicka också Authentication. För raden Windows Authentication ska status vara Enabled. Om det inte är så, högerklicka på Windows Authentication och välj Enable. (Detta gäller det vanligaste fallet, AD-autenticering och måste samspela med inställningar i web.config, se nedan.)
  - Skulle inte raden Windows Authentication alls finnas med så måste denna del först installeras:
    - Starta Server Manager, expandera Roles, klicka Web Server (IIS)
    - I mitten kan man nu gå ner en bit till Role Services
    - Under Security finns Windows Authentication
    - Ifall den är ”Not installed”:
      - Titta till höger, klicka Add Role Services, välj Windows Authentication, gör Next och Install.
    - Starta om Server Manager, annars dyker inte rollen upp i IIS-delen.

Stoppa Default Web Site, ta bort den eller byt till någon annan IP-port på den (annars funkar det inte att default på servern går till Multifraga).

Starta Multifraga-sajten om det inte redan gjorts.

(Alternativ installationsvariant: Ifall man vill ha flera sub-sajter på samma ip/port/dns-namn kan man istället starta med att under Default Web Site göra Add Application med namnet Multifraga, istället för Add Web Site en trappa upp.)

### 1.1.2. Att kopiera in distributionen (2008R2)

Vanligen får man tillgång till distributionen av en version av Multifråga som en zip-fil. Lägg den på My Documents e.dyl, öppna zip:en och kopiera alla filer/kataloger till *Multifraga\_dir*.

Aktuell kommuns logga ska även läggas in i *Multifraga\_dir/bild\_kalla/* under namnet *aktuell\_kommunlogga.jpg* (visas på startsidan).

Tips: En udda sak med Winservers filhantering är att det tycks bli olika rättigheter beroende på ifall man kopierar eller flyttar distributionens alla filer in till webbserverkatalogerna. Om man kopierar blir det rätt, ifall man flyttar måste man manuellt ändra rättigheterna (eller enklare, ta bort och kopiera istället).

### 1.1.3. Att definiera filrättigheter (2008R2)

Eftersom ASP.NET:s parameterfil *web.config* i detta fall inte tänks innehålla någon impersonate-tag (eller False) så kommer run-user för arbetstrådarna som kör ASP.NET-programmen default att vara *IIS APPPOOL\Classic .NET AppPool*. Denna special-user måste alltså ha skrivrättigheter till t.ex:

- Loggfils katalog  
(path/namn konfigureras i web.config)
- Vår temporärfils katalog för xml-svarsfiler  
(som vanligen är *Multifraga\_dir\App\_Data* även om det går att konfigurera om).

Se parametrarna *SB\_MF\_SvarsDirsPlats* och *SB\_MF\_LoggFilsPlats* i filen *web.config* (mer om den nedan).

Eftersom run-usern är lite speciell följer här en detaljerad, lånad arbetsgång för hur man sätter rätt permissions till t.ex. *App\_Data*:

1. Open Windows Explorer
2. Select a file or directory (*Multifraga\_dir\App\_Data*).
3. Right click the file and select "Properties"
4. Select the "Security" tab
5. Click the "Edit" and then "Add" button
6. Click the "Locations" button and make sure you select your machine (alltså EJ er "stora" domän).
7. Enter "*IIS AppPool\Classic .NET AppPool*" in the "Enter the object names to select:" text box.
8. Click the "Check Names" button and click "OK".

Sätt sedan Modify permissions för den usern du fick fram.  
Sedan motsvarande för loggfils katalogen.

Noteringar:

- I den äldre varianten Windows Server 2008 SP1 kör IIS istället under användaren *NETWORK SERVICE* se WinServer 2003-kapitlet nedan..
- I fallet att simpel inloggning används (se web.config-parametern MF\_Egen = ”egenskriven enkel katalog i programmet”) så blir run-usern istället nodnamn\IIS\_IUSRS.
- Om ni väljer att inte lägga webbfiler under default (C:\Inetpub\wwwroot) så är det viktigt att definiera rättigheterna Read&Exec, List, Read för både *IUSR* (verkar användas i vissa fall av systemet - kontohanteringen är mycket svårförståelig i nyare IIS) och för *IIS APPPOOL\Classic .NET AppPool*.

## 1.2. Windows Server 2003 med IIS6

### 1.2.1. Att skapa en IIS-sajt (2003)

Gå in i Admingränssnittet i Winserver2003:  
Startknappen > Administrative > IIS...

Högerklicka på Web Sites under serverdatorns namn i trädet, skapa ny site:

- Namn (description) Multifraga
- Physical path: Skapa C:\inetpub\wwwroot\Multifraga\_dir härinne, inte i vanliga Winexplorer.
- Permissions: Read + Run scripts such as ASP

Högerklicka på den nya webbsajten i trädet, välj Properties:

- Välj sedan filken ASP.NET och ASP.NET version 2.xxx (att välja v2 ger lustigt nog funktionaliteten hos även 3.0 och 3.5 i dagsläget).
- Fortfarande i Properties, välj fliken Documents och addera *default.aspx* till listan om det inte redan finns.
- Välj också fliken Directory Security, sedan Authentication and access control Edit. Välj bort anonymous, men välj Integrated Windows authentication. (Detta gäller det vanligaste fallet, AD-autentisering och måste samspela med inställningar i web.config, se nedan.)
- Samt, välj https-port under Web Site ifall säkring inte sker t.ex. med Citrix, annars http. Gå in i Directory Security, Edit, Require SSL och ange ett cert enligt kommunens normala rutiner för interna SSL-sajter.

I trädet till vänster, klicka på serverdatorns namn, dubbelklicka sedan på Web Service Extensions i högerkolumnen.

- ASP.NET v1 är förmodligen Allowed redan från början, men kanske inte Active Server Pages (som delvis betyder ASP.NET v2 - namnsättningen är inte ett under av tydlighet). Slå på Allow även på den. ASP.NET version 2.xxx ska också vara allowed.

Stoppa Default Web Site, ta bort den eller byt till någon annan IP-port på den (annars funkar det inte att default på servern går till Multifraga).

Starta Multifraga-sajten om det inte redan gjorts.

### 1.2.2. Att kopiera in distributionen (2003)

Vanligen får man tillgång till distributionen av en version av Multifråga som en zip-fil. Lägg den på My Documents e.dyl, öppna zip:en och kopiera alla filer/kataloger till *Multifraga\_dir*.

Aktuell kommuns logga ska även läggas in i *Multifraga\_dir/bild\_kalla/* under namnet *aktuell\_kommunlogga.jpg* (visas på startsidan).

Tips: En udda sak med Winservers filhantering är att det tycks bli olika rättigheter beroende på ifall man kopierar eller flyttar distributionens alla filer in till webbserverkatalogerna. Om man kopierar blir det rätt, ifall man flyttar måste man manuellt ändra rättigheterna (eller enklare, ta bort och kopiera istället).

### 1.2.3. Att definiera filrättigheter (2003)

Eftersom ASP.NET:s parameterfil *web.config* i detta fall tänks innehålla bl.a.:

```
<authentication mode="Windows"/>
```

Ingen impersonate-tag (eller False)

så kommer run-user för arbetstrådarna som kör ASP.NET-programmen default att vara *NETWORK SERVICE*. Denna special-user måste alltså ha rättigheter till t.ex. loggfilskatalog och vår temporärfilskatalog för xml-svarsfiler (som vanligen är *Multifraga\_dir\App\_Data* även om det går att konfigurera om). Se parametrarna *SB\_MF\_SvarsDirsPlats* och *SB\_MF\_LoggFilsPlats* i filen *web.config* (mer om den nedan).

Rättighetsinsättningen görs som vanligt genom högerklick på filen i Winexplorer, Properties, Security. Sätt exempelvis Full för *NETWORK SERVICE*.

I fallet att simpel inloggning används (se *web.config*-parametern *MF\_Egen = "egenskriven enkel katalog i programmet"*) så blir run-usern istället *nodnamn\IIS\_IUSRS*.

### **1.3. Att installera klient-certifikat för SHS-IWSI (ifall behövs)**

Klient-certifikat behövs endast i de fall då kommunikationen mellan webbapplikationens server och SHS-noden behöver säkras med dubbelriktad SSL (vilket betyder att både anropare och anropad har cert – detta kan förhindra man-in-the-middle-attacker etc).

Ett typfall när dubbelriktad SSL behövs är då Logicas Infratjänst anropas direkt över Internet med IWSI. Varianten kallas ”**Fjärr-IWSI**” i checklistan.

Vid egendriftning av SHS-agent, -satellit eller -nod behövs däremot vanligen inte klient-certifikat (varianten ”**Egen-IWSI**”).

Klientcertifikatet som används i detta fall är detsamma som kommunens myndighetscertifikat (även kallat organisationscertifikat) och detsamma som används i SHS. Köps normalt från Steria.

Certifikatinstallation består av ett antal steg. Det finns för övrigt ett antal beskrivningar att hitta via sökmotorer på Internet. Du behöver själva kommun-certet, dess password samt Sterias root-cert.

Här kommer ett exempel på installationsgång som befunnits fungera:

Först root-CA-certet från Steria.

1. Select Start > Run and type "mmc" to open the Microsoft Management Console (Beroende på inloggning och OS kan du behöva se till att köra som administrator)
2. Select File > Add / Remove Snap-in
3. Click the Add button
4. Select Certificates and click the Add button
5. Select Computer Account and click the Next button
6. Click the Finish button
7. Click the Close and OK buttons
8. Expand Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates
19. Right-click Certificates, point to All Tasks, and then click Import.
20. Click Next to move past the Welcome dialog box of the Certificate Import Wizard.
21. Enter the path and filename of the CA's .cer file.  
T ex *Steria\_AB\_EID\_CA\_v1.cer*
22. Click Next.
23. Select Place all certificates in the following store, and then click Browse.
24. Select Show physical stores.
25. Expand Trusted Root Certification Authorities within the list, and then select Local Computer.

26. Click OK, click Next, and then click Finish.
27. Click OK to close the confirmation message box.
28. Refresh the view of the Certificates folder within the MMC snap-in and confirm that the CA's certificate is listed.

Notering: mmc verkar även kunna importera en .p12-fil som rot-cert, men ibland kan både myndighets-cert och tillhörande rot-cert ligga i samma .p12, då verkar båda läggas in, så man kanske bör städa bort myndighets-certet sen ur rot-trädet.

Nu finns root-CA-certet nåbart från ASP.

Lägg nu in själva kommunens myndighets-cert som passar till ovanstående root-CA:

- a. To import the client certificate to the local machine store, follow these steps:  
Expand Certificates (Local Computer), and then expand Personal.
- b. Right-click Certificates, click All Task, click Import, and then click Next.
- c. In the File name box, type the file name of the cert, and then click Next.  
T ex: *shs.Botkyrka.se.p12*
- d. In the Password box, type the password that you got when ordering the cert, and then click Next two times.
- e. Click Finish, and then click OK.
- f. Refresh the view of the Certificates folder within the MMC snap-in and confirm that the client certificate is listed.
- g. Stäng mmc (du behöver inte "spara" här)

Nu ska kommun-certet vara nåbart från ASP.

Cert-filen (t ex: *shs.Botkyrka.se.p12*) ska också kopieras till en filplats där applikationskoden kan hitta den (lägg den exempelvis vid loggarna så blir det hög säkerhet plus backup på den). Ska pekas på av *SB\_MF\_KommunCertFilPath*, se nästa stycke.

Se också kapitlet om *web.config* nedan. Fälten

- *SB\_MF\_Tvavags\_SSL*
- *SB\_MF\_KommunCertFilPath* (cert-filens path)
- *SB\_MF\_KommunCertPw* (certets lösenord)

ska redigeras enligt hur ni installerat ovan.

## 1.4. Att modifiera web.config

ASP.NET:s parameterfil *web.config* (som ska ligga direkt under *Multifraga\_dir*) innehåller en mängd olika definitioner. De flesta får inte ändras utan ska vara exakt som de genererats av Visual Studio för att hela runtime-miljön ska fungera.

Andra parametrar däremot måste anpassas till kommunen och till webbservermaskinen.

När man installerar Multifråga för första gången utgår man ifrån den mall för *web.config* som följer med i distributionen. Filen har relativt omfattande kommentering som ska göra det enkelt och självförklarande att förstå vad man ska ändra på för att anpassa till aktuell miljö. Filen är i xml-format varför man måste vara kunnig i enkel xml-syntax. Filen redigeras lämpligen i Notepad. I vissa fall kan det vara trassligt att redigera på plats under *Multifraga\_dir* pga anti-hacking-skydden i Winserver 2008R2. Då kan man förstås kopiera till någon annan katalog, redigera filen och sedan kopiera tillbaka.

Framförallt är det ett antal konfigurationsparametrar för själva applikationen som ska modifieras. De ska ligga under xml-taggen `<appSettings>` och har format i stil med följande (se kommentarer i filen):

```
<add key="SB_MF_KommunOrgNr" value="2120002411"/>
```

För att få inloggning/autentisering rätt så behövs några rader i *web.config* som dessutom ska samspela med definitioner i IIS-konfigureringen. Det finns tre fall för autentisering som stöds och dessa styrs av parametern `SB_MF_Autent`, enligt följande parti lånat från en *web.config*-mall:

```
<!-- Vilken autentisering som används.
OBS! att det är mycket noga att denna parameter konfigureras
i samklang med ASP-parametrar som Windows Authent, no-anonymous etc,
se installationsvägledningen ovan.
Alternativ: "Novell"/"AD"/"MF_Egen"
Novell = eDirectory
AD = MS Active Directory
MF_Egen = egenskriven enkel katalog i programmet -->
<!-- -->
<add key="SB_MF_Autent" value="AD"/>
```

Två av varianterna är färdigutprovade i dagsläget (2010-03-03): AD och MF\_Egen. MF\_Egen bör bara användas i undantagsfall eller för test.

Följande exempel på parametersättning gäller för varianten för AD:

Under `<system.web>` i *web.config*:

```
<authentication mode="Windows"/>
<authorization>
  <allow roles="BOTKYRKA\grp-app-socmultifråga"/>
  <deny users="*/>
</authorization>
```



Dessa inställningar samverkar alltså med IIS-inställningen för autentisering enligt Integrated Windows, se avsnittet ”Att skapa en IIS-sajt” ovan.

**Funktionen blir att alla tillåtna användare ska finnas i en viss AD-grupp (i exemplet är gruppnamnet ”grp-app-socmultifråga”).** Därmed sköts lämpligen uppläggningsen av tillåtna användare av Multifråga av kommunens IT-avdelning

(Ifall varianten *MF\_Egen* ska användas ska partiet med *<authorization>* inte vara med i *web.config*.)

När *web.config* har modifierats klart är det MYCKET viktigt att kopiera filen till en kopia på något ställe där man kan återfinna den senare. Sätt gärna ett efternamn på kopian som anger när den redigerats. Orsaken är att när nästa version av Multifråga distribuerats är det lätt hänt att den mall-*web.config* som kan följa med kör över den med möda anpassade lokala filen. ASP.NET har tyvärr inte något riktigt bra mönster för att hantera programversionering och denna parameterfil.

Det är att rekommendera att inkludera modifieringshistorik i *web.config* så man kan spåra ändringar som möjligen ger problem långt senare. Gör med xml-kommentarer, t.ex enligt följande mönster:

```
<!-- #Ändr 2010-02-17 Sven-Håkan Olsson: Flyttat loggfils katalogen -->
```

## 1.5. Loggfiler

På den loggfils katalog som pekats ut av *web.config*-parametern *SB\_MF\_LoggFilsPlats* placerar applikationen två filer (om filrättigheterna är rätt satta förstås).

- *Multifraga\_Tekn\_logg.txt*
  - Tänkt för tekniker för att kunna leta efter konfigureringsfel, kommunikationstrassel, hitta felutskriften från runtime-fel, se svarstider mot de olika myndigheterna mm.
- *Multifraga\_Funk\_logg.txt*
  - Denna funktionella logg är tänkt att ge spårbarhet kring hur användarna utnyttjar applikationen och hur/vad/när de frågar myndigheterna. Missbruk är ju tänkbart eftersom det rör dig om sekretesskyddat material.
  - Kommunen bör ha en rutin så att en ”superanvändare” kan göra stickprovskontroll bland användarna för att försäkra om att inte missbruk sker.
  - Denna fil är gjord för att vara kompatibel med kalkylarksprogram som Office Excel eller OpenOffice Calc. Fälten i varje rad separeras av semikolon vilket gör att det går att importera som ”comma separated file”. Ett användningssätt är att kopiera filen, göra rename till ”.csv” och ta in den som kalkylark.
  - Loggen i sig ska betraktas som sekretessbelagd.

- Loggen ska ha backup.

För båda loggfilerna gäller:

- Om man tycker loggfilerna blir för stora för att titta i så kan man lätt göra rename till t.ex. *Multifraga\_Funk\_logg\_t\_o\_m\_2010-02-17.txt* . Sedan skapar Multifråga automatiskt en ny ”current log file”.
- Filerna kan lätt öppnas och betraktas i Notepad eller i webbläsare.
- Man kan då lätt göra ctrl-F för att söka efter något specifikt.
- Man kan också lätt göra ctrl-End för att komma till de mest aktuella loggningarna (vilka alltid appendas i slutet).

Även om det är utanför scope för denna installationsvägledning så har vanligen också den SHS-lösning man kommunicerar via mot myndigheterna loggar. Många gånger kan kommunikationstrassel bero på felkonfigurering i SHS-noden eller i brandvägg mellan webbserver och SHS-lösning, eller i brandvägg mellan SHS-lösning och Internet (i förekommande fall). Se Checklistan.

## **1.6. Felsökningstips**

Några felsökningstips:

- Vid trassel med IIS eller ASP.NET i sig, använd sökverktyg för Internet, det finns mängder med tips om installation/konfiguration.
- Autentisering, run-users och filrättighetshantering för IIS och Windows Server *är* verkligen komplext, läs på noga ifall ni väljer en annan variant än som beskrivs ovan.
- Lusläs eventuella detaljerade felutskriften på Multifrågas webbsidor. I vissa fall kan det tänkas stå intressanta saker i småramarna uppe till höger. Deras yta kan ökas genom att dra i gränslinjerna så att det går att läsa fel-infon.
- Kolla Multifrågas två egna loggar.
- Kolla SHS-lösningens administrationsgränssnitt och loggar. Ifall du köper via Infracjäst eller annan outsourcing behöver du ibland gå via deras personal.
- Läs på om kommunikationskedjan i checklistan (för dokumentnamn, se början av installationsvägledningen).
  - Dubbelkolla att alla brandväggsöppningar verkligen blivit åt rätt håll, på rätt port och eventuellt med rätt IP-avgränsning.
  - Dubbelkolla så att inte NAT/masquerading missuppfattats så att det är en annan IP-adress som ska användas.
  - Testa brandväggsöppningarna genom att provanropa från rätt ställe med telnet. Om det är en http-föribildelse som testas ska det gå att få connect och sedan slå ”GET /” och något ska komma tillbaks. Om det är https torde åtminstone initial connect ske.
  - Är det ändå mystiskt får man ansluta en IP-sniffer på olika ställen av kommunikationskedjan och testa sig fram stegvis.

- Kontakta respektiv myndighet och hör ifall de har driftsproblem, ifall de kan spåra om något anrop inkommer från oss, etc.

### **1.7. Multifråga som "slav" under verksamhetsapplikation**

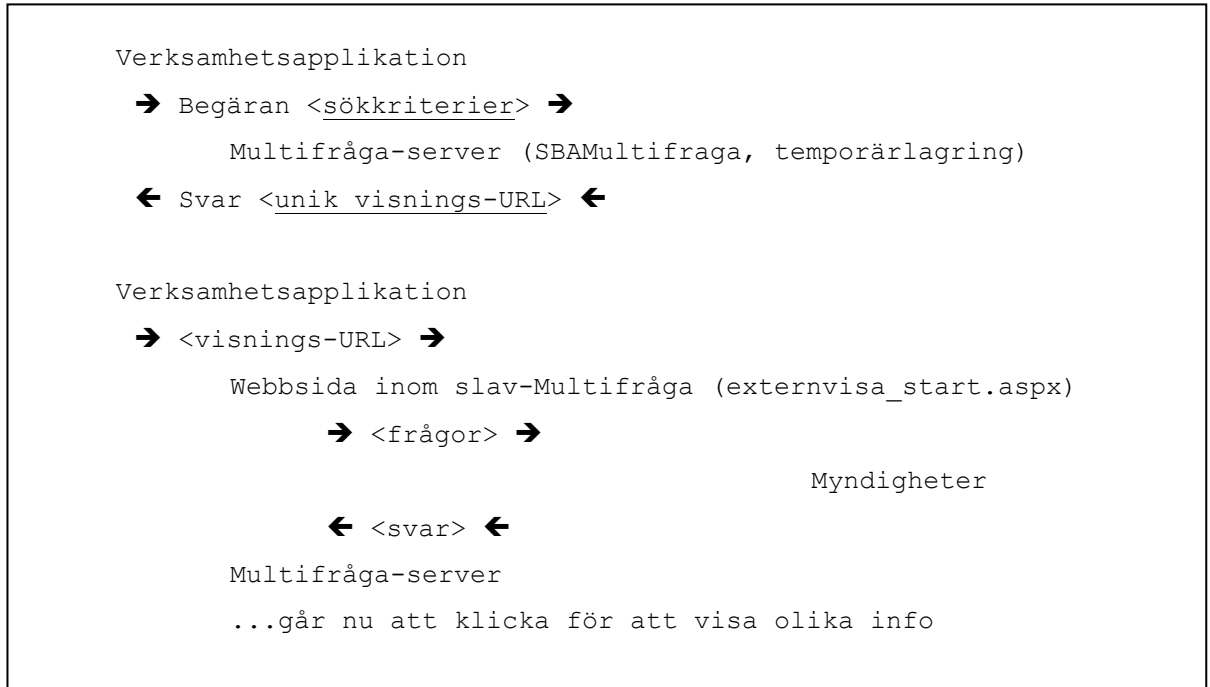
En intressant lösning är att låta en verksamhetsapplikation direkt få Multifråga att gå igång. Därmed slipper användaren mata in alla frågeparametrarna. En sådan lösning är under 2010 utvecklad i samarbete med Ilab, för deras verksamhetsapplikation Viva. I en senare fas skulle man kunna tänka sig att sedan myndighetsdata även skulle gå att automatiskt överföra till verksamhetsapplikationen, men i första läget används copy/paste för detta.

Huvudsakligen sätts Multifråga upp enligt anvisningarna ovan, men några saker skiljer:

- Om vanlig stand-alone-Multifråga också ska användas parallellt (eller under en testperiod) ska de två varianterna vara installerade i varsin webbapp eller webbsajt i IIS. De kör samma programkod men är konfigurerade olika. Troligen vill man peka på samma logg för båda instanserna.
- Skapa en webbapp eller webbsajt i IIS för slav-Multifråga enligt beskrivningarna ovan och installera programkoden för Multifråga där.
- En parameter i web.config styr att en Multifrågeinstallation ska vara slav istället för som vanligt stand-alone, sätt:  
`<add key="SB_MF_AppBeordring" value="True" />`
- En ytterligare webbapp eller webbsajt i IIS ska definieras, SBAMultifraga, enligt instruktionerna ovan.  
Dock är det alltså annan programkod som installeras här.  
Troligen vill man peka på samma logg även för denna applikation.  
Denna lilla applikation har ett enkelt REST-maskingränssnitt som verksamhetsapplikationen anropar, se dokumentet Nyttomedd\_Multifraga\_v04.doc (eller senare).
- Ifall man väljer varianten att ha flera webappar i samma websajt ska de typiskt gå mot varsin IP-port.
- Basic Authentication ska slås på för SBAMultifraga, görs i IIS Manager under IIS Authentication.  
Ifall inte detta finns valbart, se instruktionerna ovan om Add Role Services.
- Addera en lokal user i servern som ska utgöra maskin användare och "shared secret" för att verksamhetsapplikationen ska få anropa SBAMultifraga:
  - Kör mmc, add snap-in Local users and Groups

- Lägg till exempelvis "SBAMultifragaUser" med ett starkt password
- Sätt never expires och att man inte behöver ändra vid första inloggning.
- User/pw måste hanteras med sekretess. Meddela user/pw till ansvarig för verksamhetsapplikationens konfigurering, framhåll sekretessen. Meddela även url:en som SBAMultifraga får.
- Redigera in maskininloggningskraven i web.config för SBAMultifraga (shswebb i exemplet ersätts förstås med aktuellt servernamn):
  - `<authentication mode="Windows"/>`
  - `<authorization>`
  - `<allow users="shswebb\SBAMultifragaUser" />`
  - `<deny users="*" />`
  - `</authorization>`
- Ifall inte kommunikationen mellan verksamhetsapplikation och SBAMultifraga går i ett säkert nät så ska https slås på eftersom Basic Authentication ginge att sniffa.
- Testa att accessa SBAMultifraga via en webbläsare.
  - Om det är rätt ska du tvingas ange user/pw och sedan få en felsida från applikationen själv.
  - Det går också att sedan testa REST-api:et enligt Nyttomeddelandespecen med egenkonstruerade url-parametrar.
  - Svaret som visas i webbläsaren om det gått bra innehåller en visnings-url. Kopiera in denna i en webbläsare så ska själva slav-Multifråga gå igång, ställa myndighetsfrågorna och visa resultatet.

Nedanstående är lånat och modifierat från Nyttomeddelandespecen för att förtydliga, sekvensen exemplifierar kontexten som Nyttomeddelandet (understruket) används inom. Den övre delen använder SBAMultifraga, den nedre använder slav-Multifraga:



Tidssekvensen ovan kan variera eftersom de olika myndigheterna kan svara olika fort (eller möjligen inte alls, vid fel). Varje fråga är synkron men Multifråga har parallellitet t.ex. så att det inte låser sig ifall en myndighet inte ännu levererat svar när man klickar på visning.