INSTRUKTION

Datum
(Se filnamn i sidfot)

Utfärdare
Sven-Håkan Olsson

Installationsvägledning Inloggningskomponent

1. Installationsvägledning 3
1.1. Webbläsare och inloggningskomponenten 4
1.2. Vad gör egentligen inloggningskomponenten? 4
2. Kortfattad installationsanvisning för den IIS-vane 5
2.1. Komplettering för Multifråga XL (utan SAML) 6
2.2. Komplettering för Multifråga XL (med SAML) 7
3. Detaljerad installationsanvisning 9
3.1. Installation i Windows Server 9
3.1.1. Att kopiera in distributionen 10
3.1.2. Att definiera filrättigheter 10
3.2. Att modifiera web.config 11
3.3. Testa 12
3.4. Felsökningstips 12
4. Övrigt om installationen 13
4.1. Loggfiler 13
4.2. Brandvägg 13

Historik:

Datum	Beskrivning	Ändrad av
2016-08-21 v1	Första versionen	Sven-Håkan Olsson
2016-08-29 v2	Mindre tillägg	Sven-Håkan Olsson
2016-10-26 v3	Mindre tillägg	Sven-Håkan Olsson
2017-10-06 v4	Mindre tillägg för .net v4	Sven-Håkan Olsson
2019-11-18 v5	Mindre redigering och modernisering	Sven-Håkan Olsson
2023-05-30 v6	Utbyggnad av dokumentet för Multifråga XL och för SAML-varianten	Sven-Håkan Olsson
2025-04-07 v7	Några förtydliganden för SAML-fallet, mm	Sven-Håkan Olsson

Bilagor:

Nr	Beteckning	Identitet
-		

1. Installationsvägledning

Denna installationsvägledning beskriver installationen av den minimala inloggningskomponent som Sambruk skapat och som i första vändan utformats för att kunna samdrifta Multifråga på ett rationellt sätt.

För att hålla installationsvägledningen lite kortare, beskrevs hur komponenten installeras i en IIS i Windows Server 2012 R2 där ingen annan IIS-applikation finns innan. Installation i nyare versioner såsom 2016, 2019 eller 2022 är mycket lik.

Vägledningen kan eventuellt ändå uppfattas som lång, men den IIS-vane har säkert redan gjort liknande installationer ett stort antal gånger - inga "specialare" används av komponenten. Därför återfinns nedan parallellt både en mycket kort snabbvägledning (kap 2. Kortfattad installationsanvisning för den IIS-vane), och en annan mycket mer detaljerad i efterföljande kapitel.

Om komponenten ska samsas med andra IIS-applikationer (fullt rimligt eftersom komponenten drar synnerligen lite server-resurser) kan man behöva göra modifieringar i installationsgången så inte komponenten krockar med de andra applikationerna - detta handlar främst om Sites-namn etc.

I de fall komponenten delar server med andra applikationer bör det dock betonas att komponenten behöver en server som hanteras på ett väl säkrat sätt eftersom komponenten hanterar inloggning till en applikation under socialtjänstesekretess.

Andra varianter än nedan beskrivet är självfallet möjliga, IIS/ASP.NET-kunnig personal kan tänkas utforma andra lösningar baserat på serverns Windows-version, applikationskodens egenskaper och konfigurations-parametrarna.

En nyhet år 2022 var att InloggKomp nu även kan överföra roller/rättigheter i form av vissa **AD-gruppnamn** som användaren ingår i, hos kommunen. Detta infördes vid utbyggnaden av gamla Multifråga Classic till Multifråga XL. Fortfarande installeras InloggKomp således inne i kommunen. Installationsarbetet är i stort sett sig likt, men några små skillnader framgår av kap ”Komplettering för Multifråga XL (utan SAML)” nedan.

År 2023 var nyheten att det dessutom lades till möjlighet att Multifråga XL kan vara ”slav” under en **SAML v2-federation**. InloggKomp är härvid installerad i Sambruks servermiljö. Se kap ”Komplettering för Multifråga XL (med SAML)” nedan.

1.1. Webbläsare och inloggningskomponenten

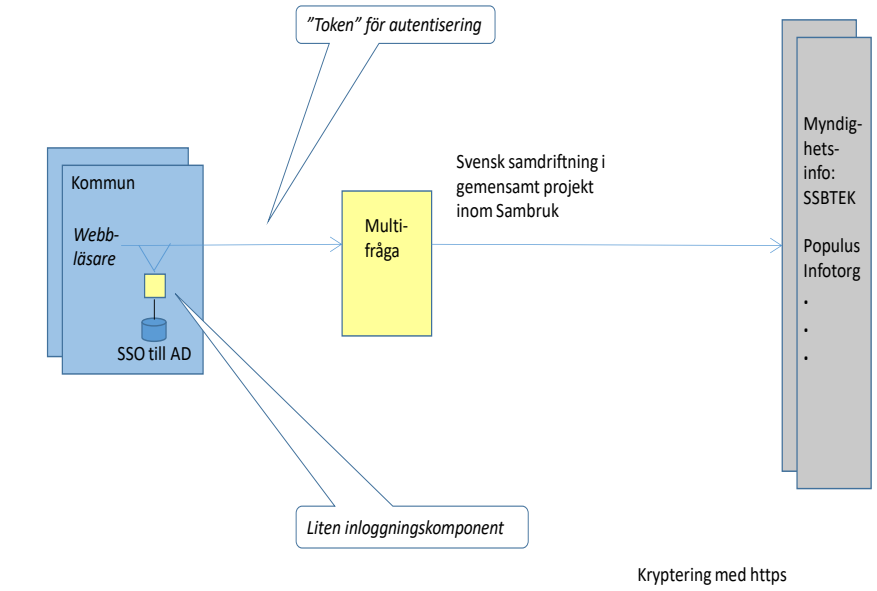
Microsoft Edge stödjer Windows Integrated Authentication som den kommuninstallerade varianten av InloggKomp behöver. Firefox och Chrome lär också gå att sätta upp för detta. Skulle inte Windows Integrated Authentication stödjas kan inloggning ske, men då får användaren upp en extra påloggningsruta där denne matar in sitt vanliga användarnamn plus lösenord relativt sitt AD.

1.2. Vad gör egentligen inloggningskomponenten?

Se även dokumentation om Multifråga.

Grundidén är helt enkelt att utnyttja en befintlig AD-autentisering inom kommunens nät, och låta den "ärvas" av Multifråga via inloggnings-komponenten och ett tokenutbyte:

Multifråga – autentisering via Sambruks InloggKomp




```
Inloggningskomponent (redan autentiserad & auktoriserad användare)
            ➔ Begäran SBAMultifragaAukt <anvandar-id...> ➔
                        (... se SBNMultifragaAuktBegar)
            ➔ Svar med start-URL-inkl-token ➔

Inloggningskomponent
            ➔ <start-URL-inkl-token> ➔
                        Multifråga startar i inloggat läge
```

2. Kortfattad installationsanvisning för den IIS-vane

- Kontrollera att IIS är normalt uppsatt, inklusive:
  - ASP.NET 3.5 (kan numera kräva sw-media)
  - Windows Authentication
  - Server Side Includes
- Skapa en Site som heter t. ex. SambrukInloggKomp, med:
  - Classic .NET AppPool.
  - Windows Authentication, EJ Anonymous Authentication.
  - Https behövs kanske inte strikt (men rekommenderas ju idag alltid att ha).
- Kopiera in InloggKomp-distributionen
- Sätt Modify-rättigheter på *App_Data*-foldern åt special-usern: *IIS AppPool\Classic .NET AppPool*
- Byt initialt namn från *web_dev.config* till *web.config* och anpassa däri (se anvisningar inne i filen - sök på **-markeringarna):
  - *<add key="SB_CF_AutentiseringsUrl"*
  - *<add key="SB_CF_AutentiseringsUser"*
  - *<add key="SB_CF_AutentiseringsPassw"*
  - *<add key="SB_MF_KommunOrgNr*
  - *<add key="SB_Multifraga_Classic_Rollnamn" value=" grp-socmultifraga ".*
  - *<allow roles="kommun-AD\grp-socmultifraga"/> t. ex*
- *Ovanstående inställningsvärden får ni i mail/sms från Sambruk.*

Vid behov, se även den detaljerade installationsanvisningen nedan.
Se även avvikelser från ovan som krävs i SAML-fallet, se nedan.

För att verifiera funktionen, lägg in dig själv temporärt i AD-gruppen (i exemplet ovan *grp-socmultifraga),* gå in på inloggningskomponentens sida, se att din user står efter "Din användaridentitet är:"och kolla att det därifrån går att komma in i den samdriftade Multifråga via knappen "Fortsätt logga in".

2.1. Komplettering för Multifråga XL (utan SAML)

Installationen är mycket lik den som beskrivs ovan, med undantag gällande några *web.config*-parametrar:

- *<add key="SB_Multifraga_XL" value="True"*
- *<add key="SB_Multifraga_XL_SAML" value="False”*
- *<add key="SB_CF_Tjanstenamn"*
  value="Samdriftad Multifråga XL Kommun A"
- *<add key=”SB_Multifraga_XL_Rollprefix” value=”MultifragaXL*”
  Detta AD-grupppprefix måste stämma med vad kommunen lägger upp för de roller/rättigheter som respektive person ska ges. Se vidare dokumentation för Multifråga XL.

Man måste komma överens med kommunen vilka AD-grupper som ska gälla och med vilket prefix.

2.2. Komplettering för Multifråga XL (med SAML)

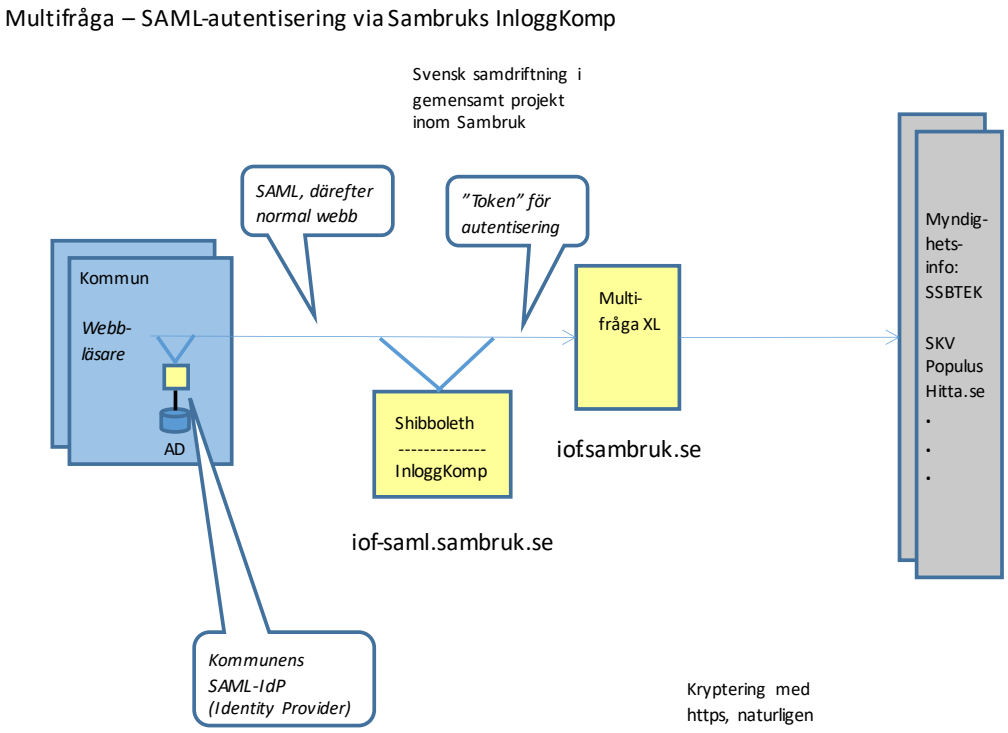
Det har nu lagts till möjlighet att Multifråga kan vara ”slav” under en SAML v2-federation, således som en SP, Service Provider.

InloggKomp agerar mellanhand för detta, som en primär SP, som sedan för över kontrollen till Multifråga såsom den verklige SP:n, via samma tokenprotokoll som från år 2022 (vilket i sin tur är mycket likt det som använts från InloggKomps början). InloggKomp är härvid installerad i Sambruks servermiljö istället för i kommunmiljön, men kommunen behöver istället förstås en SAML-”master”, dvs en IdP (Identity Provider).

InloggKomp skyddas av FOSS-programvaran Shibboleth (i sin SP-variant) som används på ett stort antal ställen, t ex på svenska universitet, kommunleverantörer mm. Det är Shibboleth som framförallt ”kan” SAML-protokollet. InloggKomp kunde därför modifieras från sin tidigare version på ett relativt enkelt sätt för att sköta även denna uppgift, framförallt som 2022-arbetet med uppdelade roller/rättigheter redan gjorts för Multifråga XL.

Man måste komma överens med kommunen vilka s.k. SAML claims som kommunen vill skicka med från sin IdP till InloggKomp via Shibboleth, Detta rör sig normalt om ett antal AD-grupper som indikerar att inlagda användare ska få vissa roller/rättigheter. Därmed är resten av överföringen från InloggKomp till Multifråga XL likadan som den som utvecklades 2022 för Multifråga XL:s rollsystem.

SAML-protokollet är tämligen komplext, nedan visas endast huvuddragen mycket schematiskt:



Installationen är mycket lik den som beskrivs överst i dokumentet, med undantag gällande några *web.config*-parametrar mm:

- *<add key="SB_Multifraga_XL" value="False"*
- *<add key="SB_Multifraga_XL_SAML" value="True”*
- *<add key="SB_CF_Tjanstenamn"*
  value="Samdriftad Multifråga XL Kommun A"
- *<add key=" SB_SAML_Identity_Provider_Value "*
  value="1234123412341234”
  Detta är identiteten i kommunens SAML-metadata som vi måste godta som bevis för dem.
- Eftersom InloggKomp i detta fall skyddas helt av Shibboleth ska det inte finnas några *Allow/Deny*-satser
- En följd av detta är att i IIS Mgr ska man endast ha Anonymous Authentication.
- Server Variables som börjar på Shib* kommer INTE med under AppPool .NET 2.0 Classic, men de kommer med under .NET 2.0 Integrated (och gissningsvis nyare).
- En följd blir alltså att Modify-rättigheter för App_Data ska sättas för run-usern *IIS APPPOOL\.NET v2.0*

Man måste också komma överens med kommunen om exakt vilka namn de vill ha på sina SAML-claims från sin IdP. Detta ska konfigureras in i Sambruks Shibboleth, främst i ATTRIBUTE-MAP.XML, men även vissa saker behöver läggas in i SHIBBOLETH2.XML, mm.
I första införandet 2023 kommer man att använda claims-namnet ”samaccountname” för användar-id samt ”memberOf” för vilka grupper användaren är med i.

3. Detaljerad installationsanvisning

3.1. Installation i Windows Server

3.1.1. Att skapa en IIS-sajt

Nedanstående skrevs initialt för Windows Server 2012 R2 (med IIS8), men skillnaderna relativt nyare versioner är små.

Kolla att ASP-rollen finns definierad för servern:

- Gå in i Server Manager
- Gå in i Add Roles på Dashboard, klicka Next i wizarden till du ser Server Roles. Expandera Web Server. Använd defaults, men:
  - Under Security, slå på Windows Authentication
  - Slå på Server Side Includes
  - Under Application Development, se till att ASP.NET 3.5 är påslaget. Eventuell får du en följdfråga om Features, acceptera.

Starta om Server Manager. I trädet till vänster, expandera IIS (alternativt starta IIS Mgr separat). I trädet i mitten, expandera ner till Sites, skapa ny sajt:

- Namn SambrukInloggKomp
- Välj application pool: *Classic .NET AppPool*
- Physical path: Skapa *C:\inetpub\wwwroot\SambrukInloggKomp* (eller annan path/namn som driften vill ha) härinne. Skapa inte i vanliga Winexplorer.
- Kommentar: Https är kanske inte strikt nödvändigt eftersom ingen hemlig info förmedlas på sträckan klientdator - inloggningskomponent (men rekommenderas ju idag alltid att ha).). Https används däremot automatiskt på sträckan inloggningskomponent - samdriftsserver men det sätts ju upp i den sistnämnda istället, liksom att https används i den påföljande kommunikationen klientdator - Multifråga.

Välj sajten i trädet och:

- Dubbelklicka IIS Authentication. För raden Windows Authentication ska status vara Enabled. Om det inte är så, högerklicka på Windows Authentication och välj Enable.

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 inloggningskomponenten).
Starta Multifraga-sajten om det inte redan gjorts.

Om inte .net v3.5 (egentl v2) skulle finnas i maskinen kan man även köra i .net v4 - v4.5. Dock finns inte *Classic .NET AppPool* då utan man får välja

DefaultAppPool. För filrättigheterna (se nedan) gäller då istället *IIS AppPool\DefaultAppPool*. Man kan också behöva kommentera bort hela *sectionGroup name="system.web.extensions"* ur *web.config*.

3.1.1. Att kopiera in distributionen

Vanligen får man tillgång till InloggKomp-distributionen av en version av inloggningskomponenten som en zip-fil. Lägg den på My Documents e.dyl, öppna zip:en, öppna InloggKomp och kopiera alla filer/kataloger till *C:\inetpub\wwwroot\SambrukInloggKomp* (eller annan path du skapade ovan).

Tips 1: En udda sak med Windows 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 gör om via kopiering istället).

Tips 2: Om man har laddat ner zip:en från en webbadress etc, kan Windows skapa en "kanske-osäker-flagga" i filattributen. Denna måste tas bort innan kopiering från zip:en sker, annars följer flaggan med till alla filerna och sajten fungerar inte. Välj zip:en > högerklick > Properties, där finns blockerings-krysset.

3.1.2. Att definiera filrättigheter

Run-user för arbetstrådarna som kör ASP.NET-programmen kommer default att vara *IIS APPPOOL\Classic .NET AppPool*. Denna special-user måste alltså ha skrivrättigheter till:

- Loggfilskatalog (som vanligen är *C:\inetpub\wwwroot\SambrukInloggKomp\App_Data* även om det går att konfigurera om i web.config, se parametern *SB_CF_LoggFilsPlats*).

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 (*...SambrukInloggKomp\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 loggfilskatalogen.

3.2. Att modifiera web.config

ASP.NET:s parameterfil *web.config* (som ska ligga direkt under foldern *SambrukInloggKomp*) 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.

Några andra parametrar däremot kan behöva anpassas till kommunen och till webbservermaskinen.

När man installerar Multifråga för första gången ska man kopiera ifrån den mall för *web.config* som heter *web_dev.config* och 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 webbroten pga anti-hacking-skydden i Winserver 2012R2. Då kan man förstås kopiera till någon annan katalog, redigera filen och sedan kopiera tillbaka.

En klassisk fälla är att *inte* ha påslaget visning av filändelser (extensions) i File Explorer. När då Notepad sparar konfigurationen blir det by default under namnet web.config.txt vilket inte i det läget framgår av visningen i File Explorer och vilket förstås inte fungerar alls.

Åtminstone är det några konfigurationsparametrar för själva applikationen som ska modifieras:

- Anropsadress (fås från Sambruk) för initialanropet som ger token
  <add key="SB_CF_AutentiseringsUrl"
- Den "shared secret" som fås från Sambruk (består av komplext par user/password)
  <add key="SB_CF_AutentiseringsUser"
  <add key="SB_CF_AutentiseringsPassw"
- Kommunens organisationsnummer:
  <add key="SB_MF_KommunOrgNr" value="212000xxxx"/>
- Aktuell AD-grupp, t ex:
  <allow roles="kommun-AD\grp-socmultifraga"/>

Dessa inställningar samverkar alltså med IIS-inställningen för autentisering enligt Integrated Windows Authentication, se ovan.
Funktionen blir att alla tillåtna användare ska finns i en viss AD-grupp (i exemplet är gruppnamnet ”grp-socmultifråga”). Därmed sköts lämpligen uppläggningen av tillåtna användare av Multifråga av kommunens IT-avdelning.

När *web.config* har modifierats klart bör man kopiera filen till något ställe där man kan återfinna den senare. Sätt gärna ett efternamn på kopian som anger när den redigerats.

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

<!-- #Ändr 2016-02-17 Sven-Håkan Olsson: Nytt logg-dir -->

3.3. Testa

För att verifiera funktionen, lägg in dig själv temporärt i AD-gruppen (i exemplet ovan *grp-socmultifraga)*, gå in på inloggningskomponentens sida, se att din user står efter "Din användaridentitet är:" och kolla att det därifrån går att komma in i den samdriftade Multifråga via inloggningsknappen.

3.4. 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 kan vara komplext, läs på noga ifall ni väljer en annan variant än som beskrivs ovan.
- Om INTE din user står efter "Din användaridentitet är:" då du provar InloggKomp så är det problem med integrerad security. Man måste normalt använda IE. Däri ska under Security det vara påslaget Enable Integrated Windows Authentication samt att det måste vara Intranet Zone (och däri påslaget Automatic Login). Detta brukar iofs vara standardinställningar. Annars kan det ha blivit fel i IIS-manager Authentication (Windows Authentication ska vara på, Anynomous Authentication ska INTE vara på).
- Lusläs eventuella detaljerade felutskrifter på inloggningskomponentens webbsidor.
- Kolla inloggningskomponentens egna logg (vanligen under foldern App_Data).
- Att testa då AD-inloggning inte riktigt fungerar på avsett sätt kan vara lite pyssligt. En hjälp kan vara att ha möjlighet att kolla exakt vad saker heter i kommunens AD-installation.
    - Exempelvis, lägg i 2012R2 till Active Directory Domain Services role i Server Manager (om den inte redan finns). Därefter är kommandoradskommandona dsquery och dsget tillgängliga, t ex:
    - C:\>dsquery group -name *grp-socmultifr**
    - C:\>dsget group -members ...

4. Övrigt om installationen

4.1. Loggfiler

På den loggfilskatalog som pekats ut av *web.config*-parametern *SB_MF_LoggFilsPlats* placerar applikationen en fil (om filrättigheterna är rätt satta förstås).

- *InloggKomp_Tekn_logg.txt*
  - Tänkt för tekniker för att kunna leta efter konfigureringsfel, kommunikationstrassel, hitta felutskrifter från runtime-fel mm.

För loggfilerna gäller:

- Backup bör finnas.
- Om man tycker loggfilerna blir för stora för att titta i så kan man lätt göra rename till t.ex. *InloggKomp_Tekn_logg_t_o_m_2016-02-17.txt* Sedan skapar Multifråga automatiskt en ny ”current log file”.
- Filerna kan lätt öppnas och betraktas i Notepad eller i webbläsare.
- Man kan då enkelt 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).

För övrigt kan nämnas att den samdriftade Multifråga har ytterligare loggning i sin server.

4.2. Brandvägg

Inloggningskomponenten behöver endast utåtgående TCP-kommunikation genom kommunens brandvägg.

Om man använder strikt filtrering i brandvägg/proxy även i det fallet så behöver https till iof.sambruk.se godkännas (port 443).

Skulle kommunen även använda interna brandvägar så behöver klientdatorerna kunna nå inloggningskomponents-servern via vanlig port 80. När inloggningen är gjord behöver klienterna kunna nå iof.sambruk.se (port 443).