SWEDISH ENVIRONMENTAL PROTECTION AGENCY

Miljöinformationsenheten (Mi)

kundtjanst@naturvardsverket.se

2019-08-22

Ärendenr:
NV-02644-17

Teknisk system-dokumentation SNA

Version P1.3

1 Basfakta

1.1 Revisionsinformation

Utgåva	Datum	Kommentar
P1.0	2018-10-22	Skapat av Lars Siden
P1.1	2018-11-08	Uppdaterad med nya brandväggsregler
P1.2	2018-11-12	Uppdaterad med konfig-värden
P1.3	2018-12-05	Uppdaterade texter

2 Bakgrund och mål

2.1 Bakgrund

För att stödja Naturvårdsverkets satsning på e-tjänster så har ett antal tekniska tjänster definierats inom SNA-projektet.

Dessa tjänster exponerar ut funktioner (även kallat API:er) som kan konsumeras maskin till maskin eller från t.ex. ett Webb GUI – så som GVU för MCP.

De tekniska tjänsterna är skapade med en Microsoft .NET teknologi som kallas WCF, Windows Communication Foundation.

WCF tekniken bygger på SOAP/XML standarden. Allt utbyte med en WCF-tjänst sker via fråga-svar mönstret. Kallas även för meddelandeorienterade tjänster.

Alla funktioner samt all information som dessa WCF tjänster erbjuder och hanterar definieras i kontrakt. Varje tjänst består av minst ett funktionskontrakt och ett informationskontrakt. Dessa kontrakt uttrycks tekniskt genom en WSDL-fil (WebService Description Language).

WSDL-filerna kan delas med konsumerande part så att de får en så kallad proxy på sin sida som innehåller listan med funktioner som tjänsten/API:t tillhandahåller plus att de informationsklasser som krävs för API-anropen kan skapas upp på den konsumerande sidan, vilket underlättar användandet av API:t samt minskar risken för fel. För test kan verktyget SoapUI användas.

API för tjänsterna beskrivs i ett annat dokument riktat mot utvecklare.

2.2 Mål

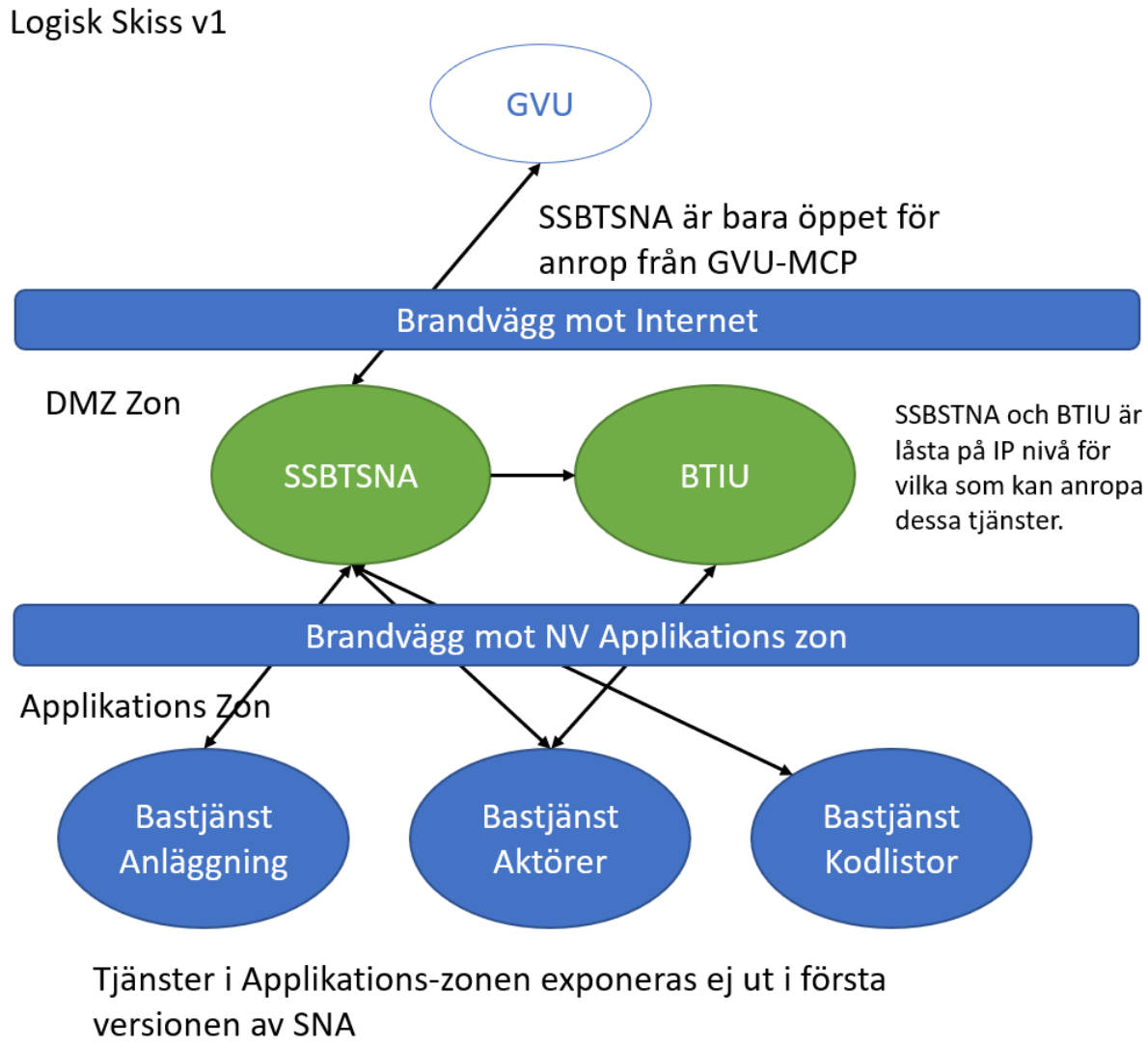
Detta dokument beskriver hur applikationen/tjänsten fungerar, ur ett tekniskt perspektiv. Det är tänkt att fungera som teknisk översiktlig beskrivning för vidareutveckling och förvaltning. APIerna och databaserna kommer beskrivas i egna dokument.

3 Gränssnitt

SNA har inget egentligt användargränssnitt utan består enbart av tekniska tjänster. Den sammanhållande tjänsten heter SSBTSNA ”Sammansatt Bastjänst Samlade Nationella Anläggningar”. Denna tjänst har via ett tjänstekontrakt ett API som kan användas av andra. Första konsument av API:t från SSBTSNA är GVU för MCP(som ligger i CGI:s e-tjänsteplattform). Hur anropen mot SSBTSNA sker från GVU-MCP är dokumenterat i dokumentet ”wireframed_förstasidan” som visar hur GVU-MCP formuläret hämtar och lämnar data mot SSBTSNA tjänsten.

4 Teknisk beskrivning

4.1 Lösningsöversikt Logisk skiss



I steg 1 av SNA projektet som skall levereras i December 2018 så byggs enbart de funktioner som krävs för MCP rapportering. För att göra anropen så enkla som möjligt så anropar SSBTSNA tjänsten BTIU(BasTjänst Inkommen Uppgift) tjänsten direkt för att lägga in informationen som en inkommen uppgift. På detta vis så får konsumenten(GVU) bara en så kallad end-point att jobba mot.

4.1.1 BTIU-Bastjänst Inlämnad Uppgift

BTIU tjänsten är ett eget förvaltningsobjekt och i det objektet finner man BTIU dokumentationen för grundtjänsten BTIU samt de tillägg som är gjorda för GVU-MCP. För SNA så används BTIU för att skicka ut den inkomna uppgiften (dvs det verksamhetsutövaren har matat in i formuläret) som e-post med bifogad PDF. BTIU skickar även samma uppgifter och PDF till den Tillsynsmyndighet som ska ta hand om ärendet. Till BTIU finns en enklare webb-söksida där man kan makulera ärenden för GVU-MCP och även skicka om mailen vid behov.

4.1.2 BTSNA(Bastjänst Anläggning)

Detta är den bastjänst som faktiskt hämtar, ändrar och lagar informationen kring anläggningar. Många av funktionerna i BTSNA och SSBTSNA är de samma.

4.1.3 BTKL(Bastjänst kodlistor)

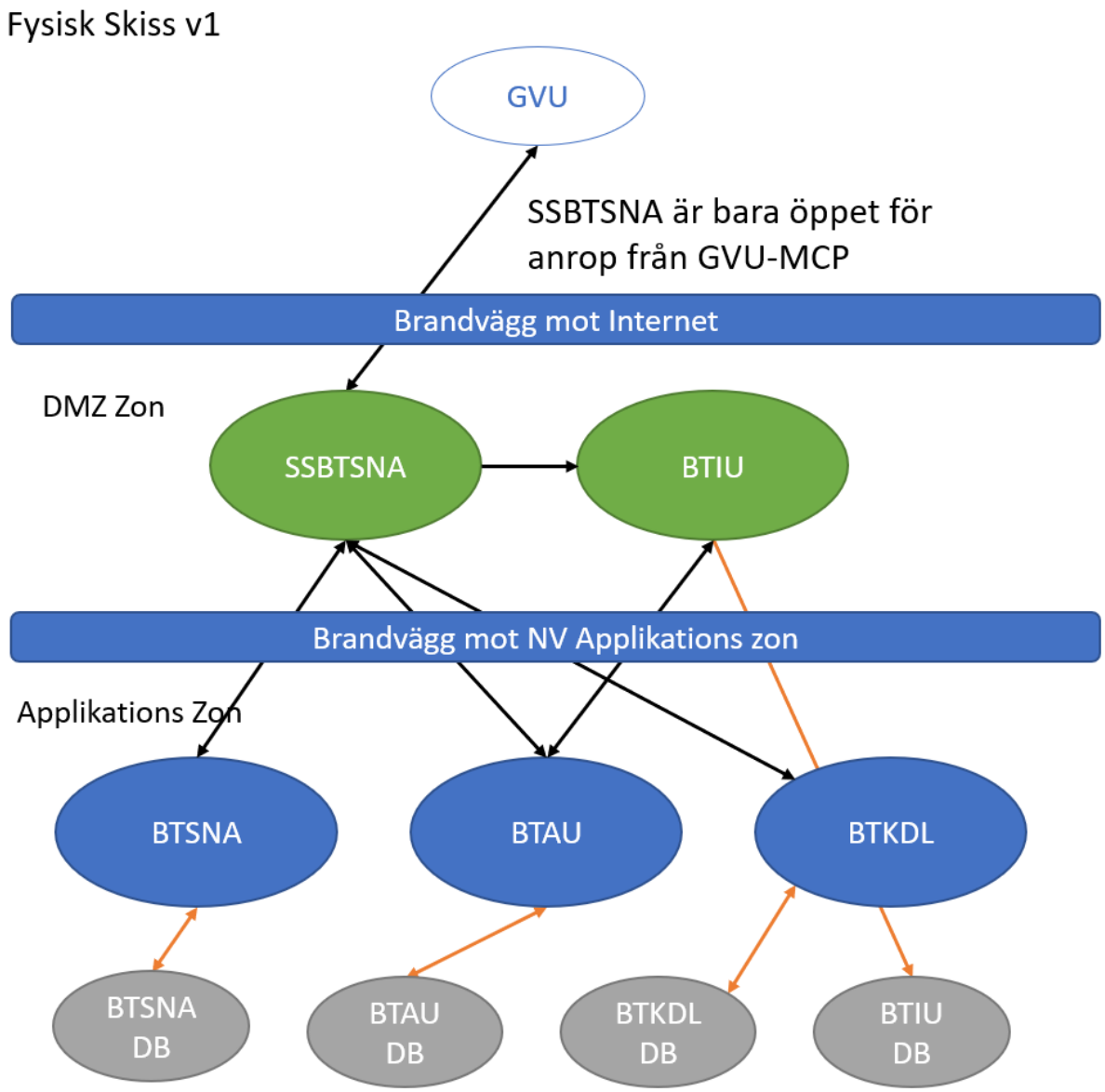
Denna bastjänst kan i dagsläget bara läsa upp information, finns inga skapa eller uppdatera metoder. Informationen i BKTKL databasen är importerad med vanliga SQL Script.

BTKL är tänkt att innehålla delad information, så som listor med branschkoder eller listor med kommuner. Strukturen av databasen för BTKL är dynamisk och flexibel. Den bygger på parent-child relationer som metadata sätts. För GVU-MCP så används den t.e.x. för listan över Tillsynsmyndigheter och listan med SNI-Koder.

4.1.4 BTAU(Bastjänst Aktörsuppgifter)

BTAU innehåller aktörer. En aktör kan vara en person eller ett företag. Tanken är att varje aktör har en uppgift kopplad till ett objekt(t.ex. en Anläggning). Detta är basen för behörighetssystemet, där vilka uppgifter man har fått sig tilldelade styr vad man får se och göra.

4.2 Lösningsöversikt – Alla komponenter



BTIU tjänsten är sedan tidigare utlagd på DMZ(men IP låst mot EF1/Plastpåse-formuläret och internt mot NV) och tanken är att den skall kunna användas av flera system på NVV. Inga databaser är exponerade direkt ut mot internet.

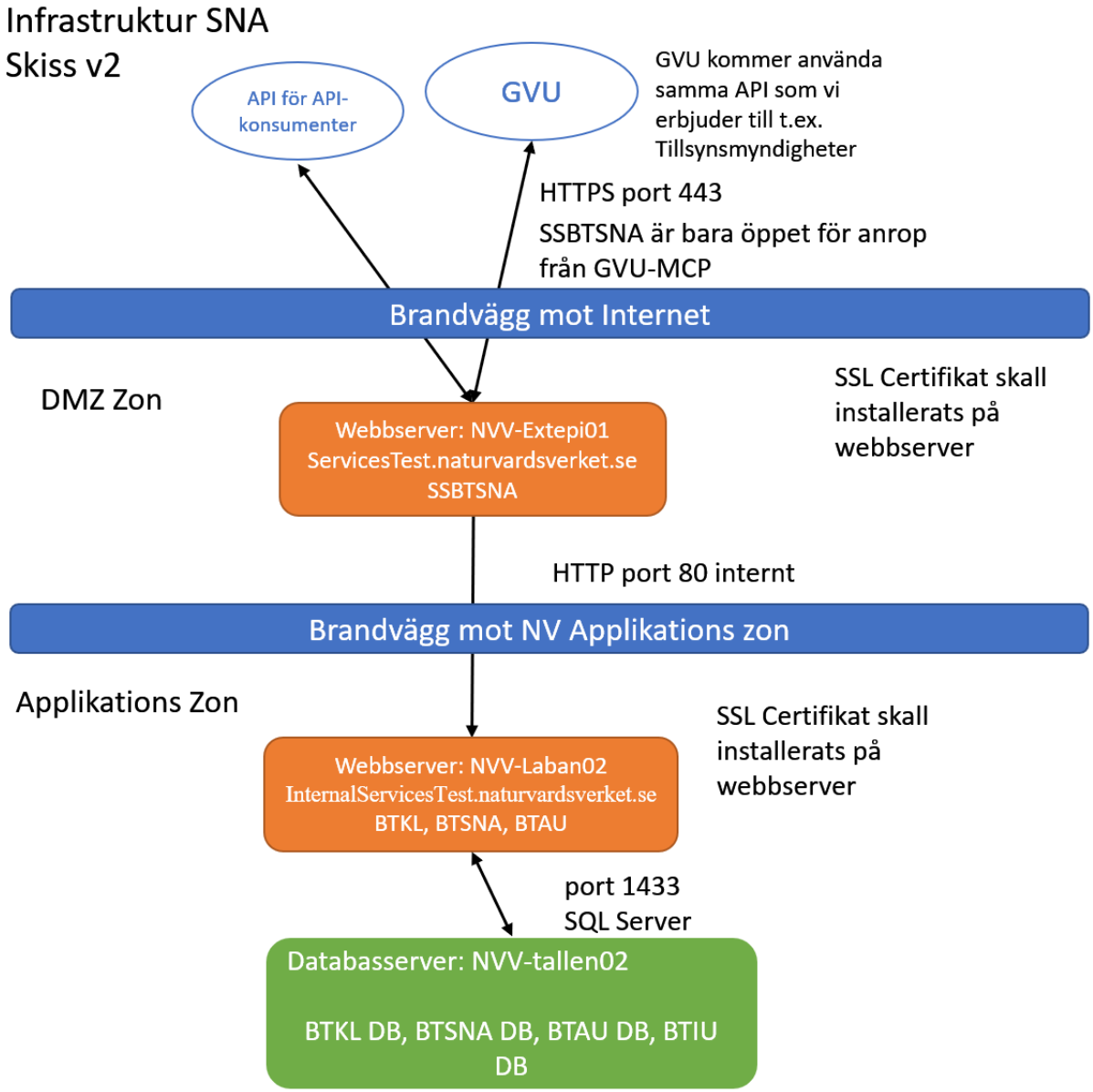
SSBTSNA har ingen egen databas utan använder de underliggande bastjänsterna för att lagra och hämta information. Varje underliggande tjänst är byggd som en svart låda enligt SOA mönstret. Orkestreringen av tjänsterna sker i SSBSTNA tjänsten – som även håller den övergripande transaktionshanteringen.

I dagsläget finns ingen maskin-till-maskin inloggning uppsatt på NV, så man har valt att låsa ner de yttre tjänsterna BTIU och SSBTSNA med IP lås så att de bara kan anropas från utvalda IP adresser.

Just nu innebär det att BTIU-tjänsten bara kan anropas inom NV nätverk, EF1/Plastpåse formulär och att BTIU-Webb bara är tillgänglig om man sitter på NV:s nät. BTIU web har vanlig username/password inloggning. BTIU kontona har en enklare rollhantering för att särskilja uppgifter från olika uppgiftslämnare.

SSBTSNA tjänsten i AT och Prod är bara exponerad mot CGI:s e-tjänsteplattform där formuläret GVU-MCP kan göra anrop.

4.3 Lösningsöversikt – Infrastruktur



Uppsättningen av tjänsterna sker på delade Windows servrar. Projektet bedömer att lasten på systemet kommer vara mycket låg till att börja med. SLA är satt till kontorstid. Inga servrar är dubblerade eller i kluster.

4.4 Tekniska förutsättningar för tjänsterna

All kod är utvecklad i Visual Studio 2017 och C# samt .Net Framework v4.6+

tekniska minimikrav:

- Windows Server 2012 eller bättre
- .Net Framwork 4.6+
- SQL Server 2012 eller bättre

Mer detaljerad information finns i ”SNA Miljöer.docx”. Vilka moduler som behöver finns installerad på servermiljön finns beskrivet i ”SNA Installationsanvisning.docx”.

4.5 Behörighet och inloggning

Behörigheten för SSBSTNA är i två lager. Det första lagret är ”Vem får anropa API:t?” och det andra lagret är ”Vilka frågor får X ställa och vilken information får X se?”. När projektet startade så höll NV på att införa ADFS/SAML och en egen IdP – så tanken var att man skulle ha en SAML-biljett för API-lagret och för ”frågelagret”. Av olika skäl så lades det projektet på is så det som är byggt nu är:

1. IP låsning för SSBTSNA tjänsten så att bara GVU-MCP formuläret kan anropa den. (för att styra vem som får anropa tjänsten/API:t)
2. Bastjänsten ”BTAU” – Aktörsregistret håller i behörigheten för vilka frågor och vad man får se. Idag så mappas BTAU behörigheten på Personnummer som kommer från BankID inloggning i GVUMCP formuläret. I BTAU knyter man sedan aktören mot olika uppgifter, dvs vilken uppgift/företag som man är kopplad till och det styr vilken behörighet man har. I framtiden så skall det byggas ett Admin GUI för BTAU så att man kan skapa aktörer som kan sköta rapporteringen för andra/flera företag/VU.

All extern kommunikation sker över SSL/HTTPS med hjälp av Naturvårdsverkets wildcard certifikat.

I projektet har det funnits tankar på klientcertifikat användning för API-säkerhet – feedback från kommuner och länsstyrelser som är kommande användare av tjänsten är att de vill använda organisationscertifikat. Inget av detta är implementerat idag.

BTAU kan enkelt byggas ut för att använda andra ID-strängar än just Personnummer om det behövs.

Alla tjänster är byggda med WCF tekniken och kan t.ex. konfigureras för att använda SAML och/eller lägga in username/password i SOAP-headern.

4.6 Admin GUI för BTAU

I första releasen av SSBTSNA / GVU för MCP så byggs inget Admin-GUI för Aktörstjänsten/registret. Ett sådant kommer behövas om t.ex Länsstyrelsen ska använda API:t i SSBTSNA direkt i sitt verksamhetssystem för då måste man kunna lägga upp användare/aktörer som får tilldelade uppgifter som visas i respektive länsstyrelses verksamhetssystem. En utökad rollhantering krävs så att en handläggare får se alla uppgifter som är kopplade till just den Tillsynsmyndigheten.

4.7 Konfiguration för tjänsternas ”web.config.”

4.7.1 Inre tjänsterna(BTAU,BTKL, BTSNA)

Konfigurationen för de inre tjänsterna är enkel. Det som är viktigt i Web.config för dessa är connect-strängarna för databasanslutningarna. Nedan är en bild på hur det är **konfigurerat i AT miljön**.

```
<connectionStrings>
  <add name="ActorDB"
    connectionString="Data Source=NVV-AT-Snake02;Initial Catalog=BTAU;Integrated Security=False;User Id=BTAUDBUser;Password=BTAU2018!;MultipleActiveResultSets=True"
    providerName="System.Data.SqlClient"/>
  <add name="PlantDB"
    connectionString="Data Source=NVV-AT-Snake02;Initial Catalog=BTSNA;Integrated Security=False;User Id=BTSNADBUser;Password=BTSNA2018!;MultipleActiveResultSets=True"
    providerName="System.Data.SqlClient"/>
  <add name="CodeListDB"
    connectionString="Data Source=NVV-AT-Snake02;Initial Catalog=BTKL;Integrated Security=False;User Id=BTKLDBUser;Password=BTKL2018!;MultipleActiveResultSets=True"
    providerName="System.Data.SqlClient"/>
</connectionStrings>
```

Här pekas databas-server samt användarnamn och lösenord ut för de databaser som tjänsterna använder. Denna information finns i **dokumentet ”SNA Installationsanvisning.docx” som ligger under kapitel 8 i leveranspaketet.**

Databas server i AT är NVV-At-Snake-02 och i produktion är det NVV-Tallen02. Namnen på konton och lösenord ska vara samma mellan AT och PROD.

4.7.2 Konfiguration yttre tjänsten SSBTSNA

För den yttre SSBTSNA tjänsten så är adresserna till de inre tjänsterna det som är viktigt att konfigurera. SSBTSNA har ingen egen databas, så det finns ingen databas-information. De som finns är URL:ar till de tre inre tjänsterna samt till BTIU tjänsten.

Här är ett exempel från AT miljön för SSBTSNA:

```
<appSettings>
  <add key="aspnet:UseTaskFriendlySynchronizationContext" value="true" />
  <add key="ActorServiceUrl" value="http://InternalServicesTest.naturvardsverket.se/Services/ActorService.svc/Services/ActorService.svc" />
  <add key="FacilityServiceUrl" value="http://InternalServicesTest.naturvardsverket.se/Services/FacilityService.svc/Services/FacilityService.svc" />
  <add key="CodeListServiceUrl" value="http://InternalServicesTest.naturvardsverket.se/Services/CodeListService.svc/Services/CodeListService.svc" />
  <add key="BTIUServiceUrl" value="https://btiu-test.naturvardsverket.se/Services/ArticleService.svc" />
</appSettings>
```

I AppSettings så pekar man ut de tre inre tjänsterna. I dagsläget så kör de inte SSL då de inte är exponerade utåt. Referensen till den fristående tjänsten BTIU läggs också in här. BTIU är tänkt att konsumeras av 3:e part och använder SSL för att kommunicera.

Finns även information om hur loggningen är inställd – exempel från AT.

```
<log4net>
  <root>
    <level value="ALL" />
    <appender-ref ref="RollingFileAppender" />
  </root>
  <appender name="RollingFileAppender" type="log4net.Appender.RollingFileAppender">
    <file value="rollingSNA.log" />
    <appendToFile value="true" />
    <rollingStyle value="Size" />
    <maxSizeRollBackups value="5" />
    <maximumFileSize value="10MB" />
    <staticLogFileName value="true" />
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%date [%thread] %level %logger - %message%newline" />
    </layout>
  </appender>
</log4net>
```

Här är inställningarna för hur mycket som skall loggas och hur loggen skall hanteras. I den andra delen av konfigurationen så lägger man till de ”lyssnare” som skall skriva ner loggen.

```
<sharedListeners>
  <add name="xml" type="System.Diagnostics.XmlWriterTraceListener" traceOutputOptions="LogicalOperationStack" initializeData="D:\logs\WCF_Messages.svclog" />
</sharedListeners>
<trace autoflush="true" />
```

Standard katalog för NV är D:\Logs

För mer information om hur loggningen kan konfigureras se: https://logging.apache.org/log4net/

5 Loggning

5.1 SSBTSNA och underliggande bastjänster - Loggning

Loggning av fel och anrop sker till fil via log4Net. Sökvägen till loggen är som standard satt till ”d:\Logs” på den maskin tjänsten är installerad på.

- Två loggningsnivåer när vi skriver till loggen; Error och Info.
- I bastjänsterna loggar vi med nivå Error om fel kastas
- I SSBTSNA loggar vi med nivå Error om fel kastas och med nivå Info för alla anropen

Person/Org-nummer loggas ej – det som loggas är ”ObjectID” och ”InstanceID” - för att kunna felsöka tjänsterna och inskickad data.

Log4Net är en open-source standardkomponent som används på många ställen. För mer information se Log4Nets projektsida:

https://logging.apache.org/log4net/

6 Miljöer

6.1 Systemtest miljö(för Softronic, nya miljöer kommer tas fram hos Consid)

SSBTSNA	https://ssbtsna-test.nvcloud.se/Services/CompositeSNAService.svc?singleWsdl
BTAU	https://ssbtsna-test.nvcloud.se/Services/ActorService.svc
BTKL	https://ssbtsna-test.nvcloud.se/Services/CodeListService.svc
BTSNA	https://ssbtsna-test.nvcloud.se/Services/FacilityService.sv
Databasserver	nv-testdb02.cloudapp.net
Kommunikation	SSBTSNA kommunicerar över port 443/SSL mot de inre bastjänsterna. I utveckling ligger dessa på samma server. De inre bastjänsterna kommunicerar över port 1433/SQL mot nv-testdb02
SSL/HTTPS	I Utveckling används certifikat från Lets Encrypt

6.2 Acceptanstest miljö(NV:s miljöer hos CGI)

SSBTSNA **NVV-ExtAtEpi01**	https://ServicesTest.naturvardsverket.se/SSBTSNA/Services/CompositeSNAService.svc
BTAU **NVV-ExtATappl01**	https://InternalServicesTest.naturvardsverket.se/Services/ActorService.svc
BTKL **NVV-ExtATappl01**	https://InternalServicesTest.naturvardsverket.se/Services/CodeListService.svc
BTSNA **NVV-ExtATappl01**	https://InternalServicesTest.naturvardsverket.se/Services/FacilityService.svc
Databasserver **NVV-AT-Snake02**	En databas per intern tjänst: BTAU,BTKL och BTSNA
Kommunikation	SSBTSNA kommunicerar över port 80 mot de inre bastjänsterna. De inre bastjänsterna kommunicerar över port 1433/SQL mot NVV-AT-Snake02. Alla anrop sker via DNS-namn om sådan ej finns så måste HOST-filen uppdateras med namn och IP-adresser.
SSL/HTTPS	I AT miljön används Naturvårdsverkets wildcard SSL Certifikat

6.3 Brandväggsregler AT

Anropande Server	Port	Målserver
nvv-extatepi01	80	**NVV-ExtATappl01**

https://ServicesTest.naturvardsverket.se		http://InternalServicesTest.naturvardsverket.se
NVV-ExtATappl01	1433	**NVV-AT-Snake02**
nvv-extatepi01 https://ServicesTest.naturvardsverket.se	443	Tillgänglig för CGI:s e-tjänsteplattform GVU-MCP via DNS namn

Se skiss under punkt 4.3

6.4 Produktions miljö(NV:s miljöer hos CGI)

SSBTSNA **NVV-ExtEpi01**	https://Services.naturvardsverket.se/SSBTSNA/Services/CompositeSNAService.svc
BTAU **NVV-Laban02**	https://InternalServices.naturvardsverket.se/Services/ActorService.svc
BTKL **NVV-Laban02**	https://InternalServices.naturvardsverket.se/Services/CodeListService.svc
BTSNA **NVV-Laban02**	https://InternalServices.naturvardsverket.se/Services/FacilityService.svc
Databasserver **NVV-Tallen02**	En databas per intern tjänst: BTAU,BTKL och BTSNA
Kommunikation	SSBTSNA kommunicerar över port 80 mot de inre bastjänsterna. De inre bastjänsterna kommunicerar över port 1433/SQL mot NVV-Tallen02. Alla anrop sker via DNS-namn om sådan ej finns så måste HOST-filen uppdateras med namn och IP-adresser.
SSL/HTTPS	I Prod miljön används Naturvårdsverkets wildcard SSL Certifikat

Anropande Server	Port	Målserver
nvv-Extepi01 https://Services.naturvardsverket.se	80	**NVV-Laban02** http://InternalServices.naturvardsverket.se
NVV-ExtATappl01	1433	**NVV-Tallen02** (databas)
nvv-ExtEpi01 https://Services.naturvardsverket.se	443	Tillgänglig för CGI:s e-tjänsteplattform GVU-MCP via DNS namn

6.5 Brandväggsregler Produktionsmiljö

Anropande Server	Port	Målserver
nvv-Extepi01 https://Services.naturvardsverket.se	80	**NVV-Laban02** http://InternalServices. naturvardsverket.se
NVV-Laban02	1433	**NVV-Tallen02** (databas)
nvv-ExtEpi01 https://Services.naturvardsverket.se	443	Tillgänglig för CGI:s e-tjänsteplattform GVU-MCP via DNS namn