

Åtkomst till SSBT

för grundläggande uppgifter om företag (SSBTGU)

för engagemang i företag (SSBTEN)

för roll i företag (SSBTRO)

för relationen företag - person (SSBTPR)

Anslutningsanvisning

Version 4.1

Innehållsförteckning

1	Ändringshistorik	3
2	Inledning.....	4
3	Översikt miljöer.....	4
3.1	Endpoints i testmiljö.....	5
3.2	Endpoints i acceptansmiljö	5
3.3	Endpoints i produktionsmiljö	6
4	Åtkomst till testmiljö	6
4.1	Öppning av brandvägg	6
4.2	Trust av Bolagsverkets servercertifikat	9
5	Åtkomst till tjänster i acceptansmiljö	10
5.1	Öppning av brandvägg	10
5.2	Trust av Bolagsverkets servercertifikat	11
5.3	Autentisering av datakonsumentens organisationscertifikat	11
5.4	Auktorisering av datakonsumenten	14
6	Åtkomst till tjänster i produktionsmiljö.....	14
6.1	Öppning av brandvägg	14
6.2	Trust av Bolagsverkets servercertifikat	14
6.3	Autentisering av datakonsumentens organisationscertifikat	15
6.4	Auktorisering av datakonsumenten	15
7	Referenser.....	15

1 Ändringshistorik

Version	Datum	Beskrivning	Ansvarig
1.0	2017-11-07	Första versionen.	Jonas Nyfeldt
2.0	2018-03-02	Uppdaterad i och med Bolagsverkets byte av domäncertifikatutfärdare till Telia.	Jonas Nyfeldt
3.0	2018-10-12	Uppdaterad med information om direkt/indirekt återanvändning.	Åsa Ekdahl
4.0	2020-05-15	Uppdaterad med information om SSBTPR. Justeringar gällande Expisoft/Steria CA.	Jonas Nyfeldt
4.1	2021-04-09	Rättning av endpoint för SSBTPR i testbanken	Erik Graeve

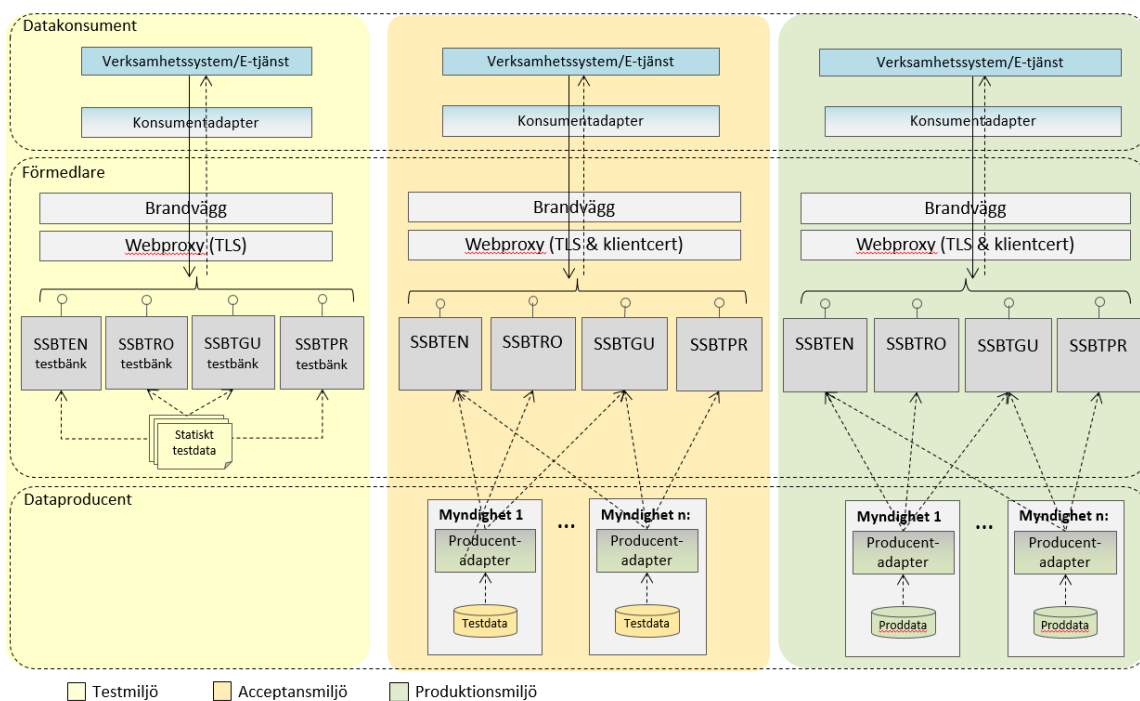
2 Inledning

Anslutning till vidareförmedlingstjänsterna SSBTEN, SSBTRO, SSBTGU och SSBTPR kräver att datakonsumenten ges åtkomst till tjänsterna i förmedlarens (Bolagsverkets) miljöer samt att datakonsumenten autentiserar sig med sitt organisationscertifikat.

Det här dokumentet syftar till att beskriva vad en datakonsument med lokal anslutning¹ behöver göra för att få åtkomst till testmiljö, acceptansmiljö och produktionsmiljö. En översikt över miljöer och hur tjänsterna skyddas finns i kapitel 3.

Vad som sedan krävs för att, i tur och ordning, ansluta till testmiljö, acceptansmiljö och produktionsmiljö beskrivs i kapitel 4, 5 och 6.

3 Översikt miljöer



Ytan med gul bakgrund till vänster i bild ger en översiktsbild av testmiljöer hos datakonsument och förmedlare. Ytan med orange bakgrund i mitten ger en översiktsbild av acceptansmiljöer hos datakonsument, förmedlare och dataproducent. Ytan med grön bakgrund till höger i bild ger en översiktsbild av produktionsmiljöer hos datakonsument, förmedlare och dataproducenter.

Hos förmedlaren visas också en brandvägg och en webproxy som en del av åtkomstkontrollen till tjänster. Brandväggar och webproxies används typiskt också hos

¹ Om datakonsumentens konsumentadapter driftas av en tredje part (till exempel som en molntjänst) ligger ansvaret att sätta upp den tekniska kommunikationen med förmedlingstjänsterna på tredjepartsleverantören. Observera att det även i ett sådant fall är datakonsumenten som ska autentiseras mot förmedlingstjänsterna, vilket innebär att tredjepartsleverantören måste använda sig av datakonsumentens certifikat vid anslutning.

datakonsumenter och dataproducenter, men hur dessa sätts upp ligger inte inom ramen för det som kan beskrivas av detta dokument och ingår därför inte heller i bilden ovan.

3.1 Endpoints i testmiljö

Följande endpoints gäller till tjänsterna i Bolagsverkets testmiljö:

SSBTEN

WSDL: <https://ssbtgu-accept2.bolagsverket.se/ssbten-dft-web/SsbtServicePorts/Test/SsbtEnTestService?wsdl>

Service: <https://ssbtgu-accept2.bolagsverket.se/ssbten-dft-web/SsbtServicePorts/Test/SsbtEnTestService>

SSBTRO

WSDL: <https://ssbtgu-accept2.bolagsverket.se/ssbtro-dft-web/SsbtServicePorts/Test/SsbtRoTestService?wsdl>

Service: <https://ssbtgu-accept2.bolagsverket.se/ssbtro-dft-web/SsbtServicePorts/Test/SsbtRoTestService>

SSBTGU

WSDL: <https://ssbtgu-accept2.bolagsverket.se/ssbtgu-dft-web-2/SsbtServicePorts/Test/SsbtTestService?wsdl>

Service: <https://ssbtgu-accept2.bolagsverket.se/ssbtgu-dft-web-2/SsbtServicePorts/Test/SsbtTestService>

SSBTPR

WSDL: <https://ssbtgu-accept2.bolagsverket.se/ssbtpr-web/SsbtprServicePorts/Test/SsbtprTestService?wsdl>

Service: <https://ssbtgu-accept2.bolagsverket.se/ssbtpr-web/SsbtprServicePorts/Test/SsbtprTestService>

3.2 Endpoints i acceptansmiljö

Följande endpoints gäller till tjänsterna i Bolagsverkets acceptansmiljö:

SSBTEN

WSDL: <https://ssbtgu-accept2.bolagsverket.se/ssbten-dft-web/SsbtServicePorts/SsbtService?wsdl>

Service: <https://ssbtgu-accept2.bolagsverket.se/ssbten-dft-web/SsbtServicePorts/SsbtService>

SSBTRO

WSDL: <https://ssbtgu-accept2.bolagsverket.se/ssbtro-dft-web/SsbtroServicePorts/SsbtroService?wsdl>

Service: <https://ssbtgu-accept2.bolagsverket.se/ssbtro-dft-web/SsbtroServicePorts/SsbtroService>

SSBTGU

WSDL: <https://ssbtgu-accept2.bolagsverket.se/ssbtgu-dft-web-2/SsbtServicePorts/SsbtService?wsdl>

Service: <https://ssbtgu-accept2.bolagsverket.se/ssbtgu-dft-web-2/SsbtServicePorts/SsbtService>

SSBTPR

WSDL: <https://ssbtqu-accept2.bolagsverket.se/ssbtp-web/SsbtpServicePorts/SsbtpService?wsdl>

Service: <https://ssbtqu-accept2.bolagsverket.se/ssbtp-web/SsbtpServicePorts/SsbtpService>

3.3 Endpoints i produktionsmiljö

Följande endpoints gäller till tjänster i Bolagsverkets produktionsmiljö:

SSBTEN

WSDL: <https://ssbtqu.bolagsverket.se/ssbten-dft-web/SsbtenServicePorts/SsbtenService?wsdl>

Service: <https://ssbtqu.bolagsverket.se/ssbten-dft-web/SsbtenServicePorts/SsbtenService>

SSBTRO

WSDL: <https://ssbtqu.bolagsverket.se/ssbtro-dft-web/SsbtroServicePorts/SsbtroService?wsdl>

Service: <https://ssbtqu.bolagsverket.se/ssbtro-dft-web/SsbtroServicePorts/SsbtroService>

SSBTGU

WSDL: <https://ssbtqu.bolagsverket.se/ssbtgu-dft-web-2/SsbtServicePorts/SsbtService?wsdl>

Service: <https://ssbtqu.bolagsverket.se/ssbtgu-dft-web-2/SsbtServicePorts/SsbtService>

SSBTPR

WSDL: <https://ssbtqu.bolagsverket.se/ssbtp-web/SsbtpServicePorts/SsbtpService?wsdl>

Service: <https://ssbtqu.bolagsverket.se/ssbtp-web/SsbtpServicePorts/SsbtpService>

4 Åtkomst till testmiljö

Eftersom tjänsterna i testmiljö enbart levererar statiska testdata behövs ingen autentisering av datakonsumenten för åtkomst. Däremot behöver Bolagsverket öppna sin brandvägg och datakonsumenten trusta Bolagsverkets utfärdare av servercertifikat för att kunna ansluta.

4.1 Öppning av brandvägg

Brandväggsöppningen beställs via SSBT@bolagsverket.se. För att lägga beställningen behöver Bolagsverket veta vilken extern IP-adress (eller vilken extern IP-adressrange) som datakonsumentens testmiljö kommer ansluta ifrån.

Som datakonsument kan man göra följande rimlighetskontroller innan beställning:

1. Säkerställa att IP-adressen/IP-adressrangen *inte* ligger inom en privat IP-adressrange. En IP-adress är privat då den ligger inom något av följande intervall:

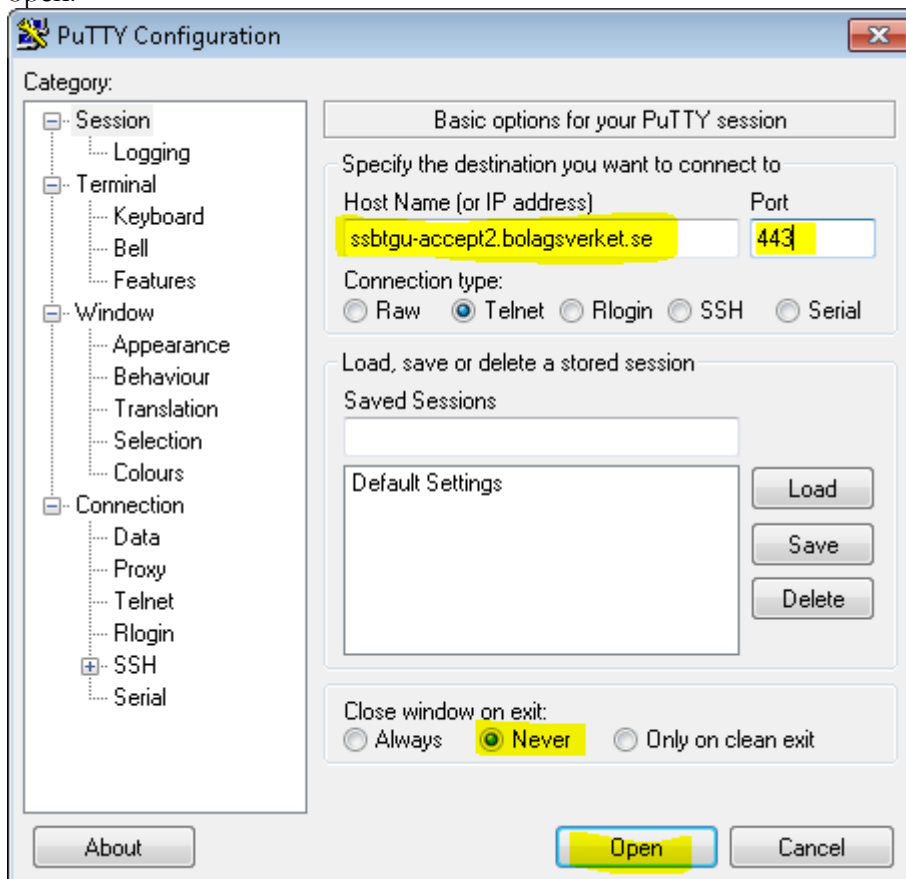
From	Tom
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

2. Använd en webläsare i testmiljön för att gå till <http://www.whatsmyip.org/> eller någon liknande tjänst. Den IP-adress som visas där ska ligga inom den IP-adressrange som beställningen gäller.

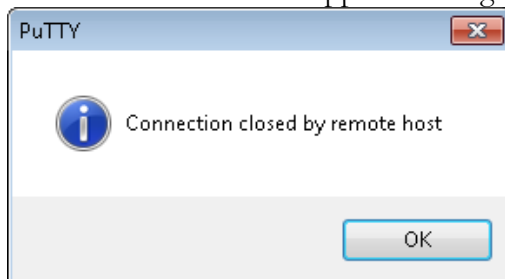
När Bolagsverkets kontaktperson meddelar att brandväggsöppningen är klar kan datakonsumenten verifiera det genom att göra en telnet-uppkoppling till:

- Host: ssbtgu-accept2.bolagsverket.se
- Port: 443

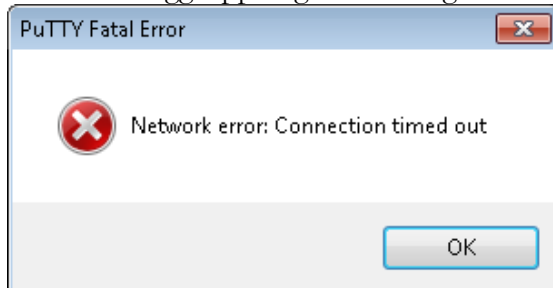
Exempel med Putty (<http://www.putty.org/>) som klient: Mata in följande och tryck på open:



Om datakonsumenten släpps in i Bolagsverkets testmiljö visar Putty följande dialog:



Om brandväggsöppningen inte fungerat visar Putty följande dialog (efter en stund):



Vid fel kontrollera först att korrekt host och port används, att trafiken släppts ut genom datakonsumentens brandväggar samt att datakonsumentens externa IP-adress stämmer med beställningen. Om det fortfarande inte fungerar, ta kontakt med kontaktperson på Bolagsverket för hjälp med felsökning.

4.2 Trust av Bolagsverkets servercertifikat

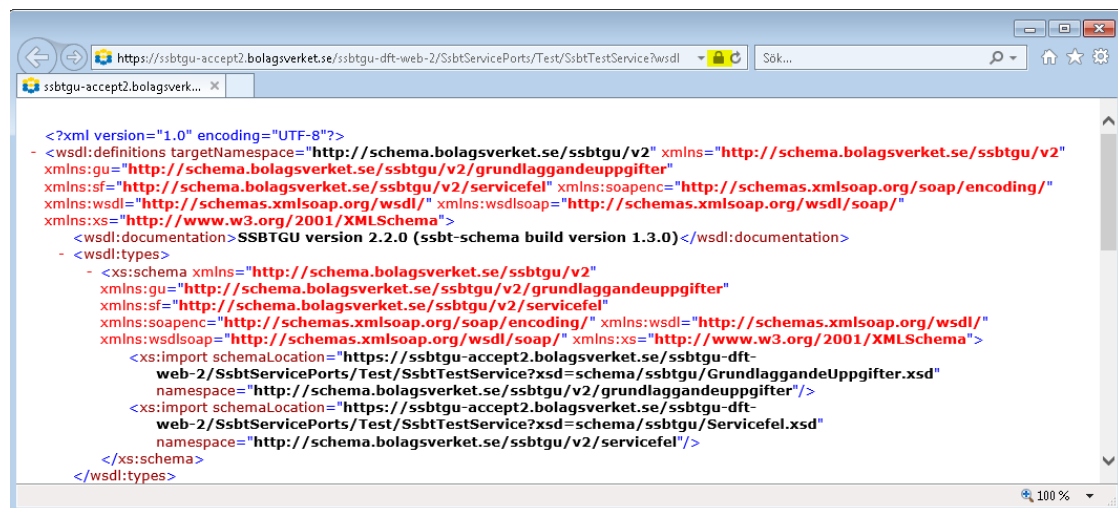
I testmiljö använder sig Bolagsverket av ett servercertifikat med följande DN:

```
CN = *.BOLAGSVERKET.SE, OU = IT, O = Bolagsverket, L = SUNDSVALL, C = SE
```

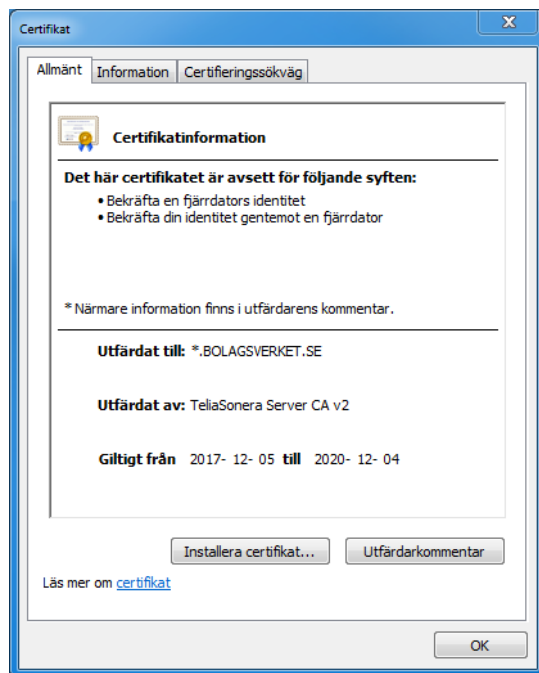
Bolagsverkets servercertifikat är ett ”domain validation certificate” utfärdat av Telia Sonera. För att kunna kommunicera med Bolagsverket via https måste datakonsumenten därför trusta certifikat utfärdare med följande rootcertifikat:

```
CN = TeliaSonera Root CA v1, O = TeliaSonera
```

Eftersom vanliga webbläsare, såsom Internet Explorer, Firefox och Chrome, har detta rootcertifikat förinstallerat, är det bra att som datakonsument först verifiera att webbläsaren kommer åt någon av WSDL:erna som publiceras av tjänsterna i förmedlarens testmiljö. Ett exempel med <https://ssbtgu-accept2.bolagsverket.se/ssbtgu-dft-web-2/SsbtServicePorts/Test/SsbtTestService?wsdl> och webbläsaren Internet Explorer 11 visas nedan:



Visar webbläsaren WSDL:en som i exemplet ovan är det ett bevis på att webbläsaren trustar Bolagsverkets servercertifikat. Genom att klicka på hänglåset (markerat med gult i bilden ovan) och välja ”Visa certifikat” kan man se Bolagsverkets aktuella certifikatsuppgifter:



En konsumentadapter som vill ansluta till testmiljön eller acceptansmiljön behöver se till att Telia Soneras rootcertifikat finns installerat i konsumentadapterns truststore. Rootcertifikatet kan laddas ned här:

<https://repository.trust.teliasonera.com/teliasonerarootcav1.cer>

Skulle en konsumentadapter försöka ansluta till testmiljön utan att trusta rätt rootcertifikat kommer anslutningen misslyckas. Hur detta misslyckande manifesterar sig varierar mellan olika tekniska plattformar. Nedan följer ett exempel på en exception som indikerar detta fel för en konsumentadapter implementerad i java:

```
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
```

5 Åtkomst till tjänster i acceptansmiljö

Tjänsterna i acceptansmiljö levererar dynamiska testdata från respektive dataproducent på motsvarande sätt som i produktion. Därför behövs ytterligare autentisering och auktorisering av datakonsumenten ske för att ge åtkomst till tjänsterna. Däremot behövs ingen ytterligare brandväggsöppning eller trust av certifikat eftersom samma brandvägg och certifikat gäller både för testmiljön och acceptansmiljön.

5.1 Öppning av brandvägg

Ingen ytterligare brandväggsöppning behövs.

5.2 Trust av Bolagsverkets servercertifikat

Samma servercertifikat som används i testmiljö enligt kapitel 4.2 används också i acceptansmiljön.

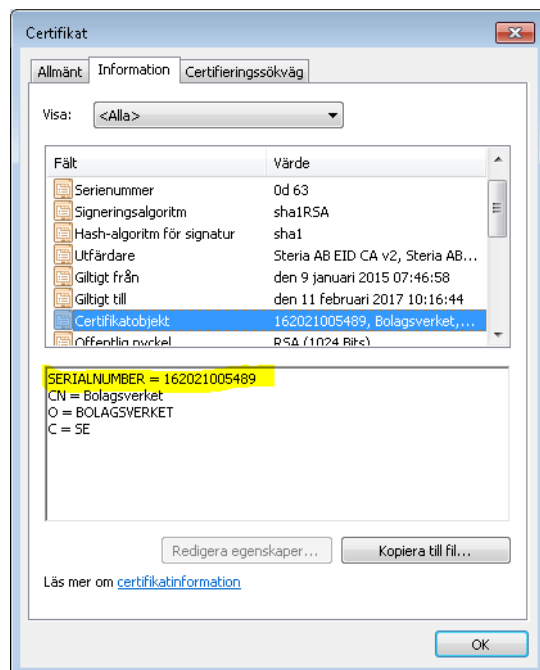
5.3 Autentisering av datakonsumentens organisationscertifikat

Konsumentadaptorn (och/eller eventuella webproxies hos datakonsumenten) måste konfigureras så att ett organisationscertifikat utfärdat av Expisoft/Steria skickas med i TLS-handskakningen med tjänsterna. Organisationscertifikatet ska vara utfärdat med rootcertifikat för Expisoft/Steria för test- eller produktionsbruk med något av nedanstående DN:

- `CN=ExpiTrust Test CA v8,O=Expisoft AB,C=SE`
- `CN=ExpiTrust test CA v7,O=Expisoft AB,C=SE`
- `CN=ExpiTrust EID CA v4,O=Expisoft AB,C=SE`
- `CN=Steria AB EID CA v2,O=Steria AB,C=SE`

Formuleringen ”utfärdat med rootcertifikat” avser att det finns en obruten kedja av giltiga certifikat från organisationscertifikatet till rootcertifikatet med ovanstående DN.

Organisationscertifikatet måste innehålla ett SERIALNUMBER med datakonsumentens 10-siffriga organisationsnummer prefixat med 16 i certifikatets DN, se exemplet nedan som visar Bolagsverkets egna organisationscertifikat utfärdat av Expisoft/Steria:



Certifikatet måste också vara giltigt, så certifikatet i exemplet ovan fungerar inte efter 2017-02-11.

Om datakonsumenten redan har integrationer med myndigheters tjänster, till exempel Navet hos Skatteverket, är det sannolikt att datakonsumenten redan har ett organisationscertifikat utfärdat av Expisoft/Sterea som går att använda även mot SSBT. Om inte, kan organisationscertifikat (eller serverlegitimation/organisationslegitimation som det kallas hos Expisoft) beställas via <https://eid.expisoft.se/valj-elegitimation/>. Serverlegitimationen måste minst ha användningssyftet ”identifiering av kund (vem som kopplar upp sig till en e-tjänst)” enligt information på beställningssidan. Att ha fler användningssyften, till exempel också ”identifiering av server”, fungerar också. Ett certifikat som används i syftet ”client authentication” kallas också klientcertifikat.

Vid korrekt uppsatt organisationscertifikathantering hos datakonsumenten ska en SOAP-request till någon av tjänsterna, till exempel till SSBTEN <https://ssbtgu-accept2.bolagsverket.se/ssbten-dft-web/SsbtenServicePorts/SsbtenService>, passera webproxyn och nå fram till tjänsten.

En exempelrequest där Bolagsverket (organisationsnummer 2021005489) agerar datakonsument med en e-tjänst med namnet TEST:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body>
    <eng:EngagemangBegaran xmlns:eng="http://schema.bolagsverket.se/ssbten/engagemang"
      xmlns:met="http://schema.bolagsverket.se/ssbt/metadata"
      xmlns:for="http://schema.bolagsverket.se/ssbt/foretag" SchemaVersion="1.3.0">
      <eng:EngagemangBegaranMetadata>
        <met:MeddelandeId>0bfeb944-aa62-42af-afbd-c9f749b2d5c4</met:MeddelandeId>
        <met:TransaktionId>fb21b9c9-2285-42d6-b66d-365e3651807e</met:TransaktionId>
        <met:Tidstempel>2017-03-17T14:16:31.310Z</met:Tidstempel>
        <met:Datakonsument>
          <met:PartId>
            <met:Organisationsnummer>2021005489</met:Organisationsnummer>
          </met:PartId>
          <met:PartNamn>Bolagsverket</met:PartNamn>
          <met:Service>
            <met:ServiceNamn>TEST</met:ServiceNamn>
          </met:Service>
        </met:Datakonsument>
        <met:Anvandare>
          <met:PartId>
            <met:Personnummer>198001011234</met:Personnummer>
          </met:PartId>
          <met:PartNamn>Jon Doe</met:PartNamn>
        </met:Anvandare>
        <met:Anvandningsomrade>IndirektAteranvandning</met:Anvandningsomrade>
      </eng:EngagemangBegaranMetadata>
      <eng:EngagemangBegaranDetaljer>
        <eng:PersonId>
          <for:PersonIdentitetsbeteckning>
            <for:Personnummer>198001011234</for:Personnummer>
          </for:PersonIdentitetsbeteckning>
        </eng:PersonId>
        <eng:Foretagsformer>
          <for:ForetagsformKod>AB</for:ForetagsformKod>
        </eng:Foretagsformer>
      </eng:EngagemangBegaranDetaljer>
    </eng:EngagemangBegaran>
  </soapenv:Body>
</soapenv:Envelope>
```

Om autentiseringen lyckas svarar SSBTEN med ett Servicefel i ett SOAP-fault:

```
<Envelope xmlns="http://schemas.xmlsoap.org/soap/envelope/">
  <Body>
    <Fault>
      <faultcode>soap:Server</faultcode>
      <faultstring>Access inte tillåten</faultstring>
      <detail>
        <sf:Servicefel xmlns:sf="http://schema.bolagsverket.se/ssbten/servicefel"
          xmlns:fel="http://schema.bolagsverket.se/ssbt/fel"
          xmlns:met="http://schema.bolagsverket.se/ssbt/metadata"
          SchemaVersion="1.3.0">
          <sf:ServicefelMetadata>
            <met:MeddelandeId>05c0896a-027c-49a1-8d75-ea183d5df07a</met:MeddelandeId>
            <met:TransaktionId>fb21b9c9-2285-42d6-b66d-365e3651807e</met:TransaktionId>
            <met:Tidstempel>2017-08-04T15:15:01.902+02:00</met:Tidstempel>
            <met:Datakonsument>
              <met:PartId>
                <met:Organisationsnummer>2021005589</met:Organisationsnummer>
              </met:PartId>
              <met:PartNamn>Bolagsverket</met:PartNamn>
              <met:Service>
                <met:ServiceNamn>TEST</met:ServiceNamn>
              </met:Service>
            </met:Datakonsument>
            <met:Anvandare>
              <met:PartId>
                <met:Personnummer>194806261691</met:Personnummer>
              </met:PartId>
              <met:PartNamn>Jon Doe</met:PartNamn>
            </met:Anvandare>
            <met:Formedlare>
              <met:PartId>
                <met:Organisationsnummer>2021005489</met:Organisationsnummer>
              </met:PartId>
              <met:PartNamn>Bolagsverket</met:PartNamn>
              <met:Service>
                <met:ServiceNamn>Bolagsverket</met:ServiceNamn>
              </met:Service>
            </met:Formedlare>
          </sf:ServicefelMetadata>
          <sf:ServicefelDetaljer>
            <fel:Fel Kalla="Formedlare" Typ="OgiltigBegaran">
              <fel:FelBeskrivning>Access inte tillåten</fel:FelBeskrivning>
            </fel:Fel>
          </sf:ServicefelDetaljer>
        </sf:Servicefel>
      </detail>
    </Fault>
  </Body>
</Envelope>
```

Att tjänsten returnerar ”Access inte tillåten” är förväntat så länge som vi inte auktoriserat datakonsumenten enligt kapitel 5.4, men förekomsten av ett SOAP-fault visar att datakonsumenten klarat webproxyns autentiseringskontroll med hjälp av sitt organisationscertifikat. Om autentiseringskontrollen av datakonsumenten misslyckas, kommer konsumentadaptern istället se någon form av TLS-handskakningsfel. Nedan följer ett exempel på en exception som indikerar ett sådant fel för en konsumentadapter implementerad i java:

```
javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure
```

Vid fel kontrollera först att åtkomst enligt kapitel 5.1 och 5.2 fortfarande fungerar, samt att ett organisationscertifikat enligt ovan skickas med i TLS-handskakningen mot

Bolagsverkets tjänster. Om det fortfarande inte fungerar, ta kontakt med kontaktperson på Bolagsverket för hjälp med felsökning.

5.4 Auktorisering av datakonsumenten

Sista steget för åtkomst till tjänsterna är att auktorisera datakonsumenten och dess e-tjänst(er)/verksamhetssystem. Auktorisering beställs via kontaktperson på Bolagsverket. Beställningen ska innehålla datakonsumentens 10-siffriga organisationsnummer och ett servicenamn för de e-tjänster/verksamhetssystem som ska anslutas. Det 10-siffriga organisationsnumret måste vara detsamma som de 10 sista siffrorna i organisationsnumret i organisationscertifikatet.

När Bolagsverkets kontaktperson meddelar att beställningen registrerats kan datakonsumenten verifiera det genom att köra samma SOAP-request som i kapitel 5.3. Om auktoriseringen lyckas svarar SSBTEN med ett EngagemangSvar:

```
<Envelope xmlns="http://schemas.xmlsoap.org/soap/envelope/">
  <Body>
    <eng:EngagemangSvar xmlns:eng="http://schema.bolagsverket.se/ssbten/engagemang"
      xmlns:fel="http://schema.bolagsverket.se/ssbt/fel"
      xmlns:met="http://schema.bolagsverket.se/ssbt/metadata"
      xmlns:for="http://schema.bolagsverket.se/ssbt/foretag" SchemaVersion="1.3.0">
      ...
    </eng:EngagemangSvar>
  </Body>
</Envelope>
```

Misslyckas auktoriseringen svarar SSBTEN med ett Servicefel som i kapitel 5.3. Vid Servicefel kontrollera först att organisationssnumret och servicenamnet som skickas i SOAP-requestens metadata överensstämmer med det som angivits i beställningen, samt att organisationsnumret överensstämmer med organisationscertifikatets organisationsnummer. Om det fortfarande inte fungerar, ta kontakt med kontaktperson på Bolagsverket för hjälp med felsökning.

6 Åtkomst till tjänster i produktionsmiljö

Tjänsterna i produktionsmiljö levererar riktiga data från respektive producent. Därför behövs ytterligare autentisering och auktorisering av datakonsumenten ske för att ge åtkomst till tjänsterna.

6.1 Öppning av brandvägg

Ingen ytterligare brandväggsöppning behövs.

6.2 Trust av Bolagsverkets servercertifikat

Samma servercertifikat som används i testmiljö enligt kapitel 4.2 används också i produktionsmiljö.

6.3 Autentisering av datakonsumentens organisationscertifikat

Konsumentadaptern (och/eller eventuella webproxies hos datakonsumenten) måste även i produktionsmiljö konfigureras så att ett organisationscertifikat utfärdat av Expisoft/Steria skickas med i TLS-handskakningen med tjänsterna.

Organisationscertifikatet ska vara utfärdat med rootcertifikat för Expisoft/Steria för produktionsbruk med något av nedanstående DN:

- `CN=ExpiTrust EID CA v4,O=Expisoft AB,C=SE`
- `CN=Steria AB EID CA v2,O=Steria AB,C=SE`

6.4 Auktorisering av datakonsumenten

Samma auktorisering av datakonsumenten och dess e-tjänst(er) som gjordes i testmiljö enligt kapitel 5.4 måste också göras i produktionsmiljö. Även denna auktorisering beställs via kontaktperson på Bolagsverket och kan testas på motsvarande sätt som beskrivits i kapitel 5.4.

7 Referenser

Dokumentation finns tillgänglig på Bolagsverkets webbplats, www.bolagsverket.se/sammansatt-bastjanst.