

Anslutningsanvisning för åtkomst till SSBTGO Notifiering

Sammansatta bastjänsten för
grunddata om organisationer

Version: 1.0

Innehållsförteckning

1	Ändringshistorik	3
2	Summering	4
3	Inledning.....	4
4	OpenAPI-specifikation	5
5	Access token	5
5.1	Validering av klientcertifikat	6
5.2	Generera access token från applikation	7
6	URL:er för API-resurser	8
7	Exempel.....	9
7.1	Generera en access token (klientcertifikat)	9
7.2	Generera en access token (utan certifikat)	9
7.3	Återkalla en access token (utfärdad utan certifikat)	10
7.4	Anropa resurs "isalive"	10
7.5	Ytterligare exempel	10

1 Ändringshistorik

Version	Datum	Beskrivning	Ansvarig
1.0	2024-05-16	Anslutningsanvisning för åtkomst till SSBTGO-Notifiering.	SSBTGO-teamet

2 Summering

- Access token URL invoke med klientcertifikat (produktion):
https://sysorgauth.bolagsverket.se/auth/realms/sysorg/protocol/openid-connect/token?client_id=<client_id>
- Access token URL invoke utan certifikat (produktion):
<https://portal.api.bolagsverket.se/oauth2/token>
- Access token URL revoke med klientcertifikat (produktion):
<https://sysorgauth.bolagsverket.se/auth/realms/sysorg/protocol/openid-connect/revoke>
- Access token URL revoke utan certifikat (produktion):
<https://portal.api.bolagsverket.se/oauth2/revoke>
- Access token URL invoke med klientcertifikat (test):
https://sysorgauth-accept2.bolagsverket.se/auth/realms/sysorg/protocol/openid-connect/token?client_id=<client_id>
- Access token URL invoke utan certifikat (test):
<https://portal-accept2.api.bolagsverket.se/oauth2/token>
- Access token URL revoke med klientcertifikat (test):
<https://sysorgauth-accept2.bolagsverket.se/auth/realms/sysorg/protocol/openid-connect/revoke>
- Access token URL revoke utan certifikat (test):
<https://portal-accept2.api.bolagsverket.se/oauth2/revoke>
- Header prefix: Bearer
- Autentiseringsmetod (grant type): Client Credentials (i kombination med klientcertifikat om så önskas)
- Auktorisation för att hämta token: Basic Auth Header
- Auktorisation för att anropa API: Bearer Auth Header
- Scopes: ssbtago-notifiering:read & ssbtago-notifiering:ping
- DevPortal URL (produktion):
<https://portal.api.bolagsverket.se/devportal/apis>
- Request URL (produktion):
<https://gw.api.bolagsverket.se/ssbtgo-notifiering/{version}/{endpoint}>
- Request URL endpoint is alive (produktion):
<https://gw.api.bolagsverket.se/ssbtgo-notifiering/v1/isalive>
- DevPortal URL (test):
<https://portal-accept2.api.bolagsverket.se/devportal/apis>
- Request URL (test):
<https://gw-accept2.api.bolagsverket.se/ssbtgo-notifiering/{version}/{endpoint}>
- Request URL endpoint is alive (test):
<https://gw-accept2.api.bolagsverket.se/ssbtgo-notifiering/v1/isalive>

3 Inledning

Anslutning till det REST API som "SSBTGO Notifiering" erbjuder kräver att datakonsumenten ges åtkomst till tjänsten i Bolagsverkets miljöer samt att datakonsumenten autentiserar sig med så kallad "access token".

API "SSBTGO Notifiering" är det gränssnitt som nyttjas för att som datakonsument administrera de prenumerationer man önskar, det vill säga vilka organisationsnummer man vill ha notifieringar om vid uppdateringar. Vid utveckling av en ny klient som ska lyssna på själva notifieringarna kan man med fördel nyttja API "SSBTGO Notifiering-Utv" för att initiera utskick av testmeddelanden.

Det här dokumentet syftar till att beskriva de delar en datakonsument behöver känna till för att upprätta anslutning mot API "SSBTGO Notifiering" i testmiljö ("accept2") och produktion.

4 OpenAPI-specifikation

En fullständig specifikation över API:et finns beskriven enligt OpenAPI 3.0.3. Följ stegen nedan för att ladda ner denna:

- Gå till Bolagsverkets WSO2 DevPortal:
 - Produktion: <https://portal.api.bolagsverket.se/devportal/apis>
 - Test: <https://portal-accept2.api.bolagsverket.se/devportal/apis>
- Klicka på API "SSBTGO Notifiering".
- Om man föredrar en Swagger-fil:
 - Klicka på "Download Swagger" nere till höger, under rubrik "Source".
- Om man föredrar en Postman Collection:
 - Klicka på "Try Out" i vänstermenyn och därefter på "POSTMAN COLLECTION" under stycke "Gateway".
- Swagger-filen kan med fördel användas för att generera klientkod.

5 Access token

Tjänsten är publicerad på Bolagsverkets API-portal vilken bygger på WSO2 API Manager. Denna nyttjar JSON Web Token (JWT) för autentisering.

Det finns två olika endpoints man kan nyttja för att generera en access token – båda två följer ett "Client Credentials"-flöde men den ena tillämpar dessutom "mutual TLS" i kombination med client credentials och kräver att man autentiserar sig med ett klientcertifikat vilket är rekommenderat. Se mer under kapitel 5.1 Validering av klientcertifikat.

Värden för "client_id" och "client_secret" levereras till datakonsumenten via mail som en krypterad zip-fil när denna tilldelas åtkomst i Bolagsverkets miljö. Lösenordet levereras separat i ett SMS. Observera att om man ska använda sig av ett klientcertifikat behövs ingen "client_secret" utan detta fält lämnas då tomt i anropet. Däremot ska ett alternativt "client_id" användas, som dessutom måste skickas med som en query-parameter i den token-URL som gäller för klientcertifikat (se länkar nedan, ersätt "<client_id>" med den identitet som ska gälla). Detta alternativa "client_id" levereras i ett separat mail med ytterligare instruktioner för klientcertifikat.

Giltighetstiden för en access token är begränsad och måste genereras dynamiskt av klientens applikation. Notera att API:et dessutom skyddar sina resurser med "scopes", dessa måste anges i anropet när man hämtar en ny token.

URL för att hämta token med hjälp av klientcertifikat (produktion):

https://sysorgauth.bolagsverket.se/auth/realms/sysorg/protocol/openid-connect/token?client_id=<client_id>

URL för att hämta token med hjälp av klientcertifikat (test): https://sysorgauth-accept2.bolagsverket.se/auth/realms/sysorg/protocol/openid-connect/token?client_id=<client_id>

URL för att hämta token utan certifikat (produktion):

<https://portal.api.bolagsverket.se/oauth2/token>

URL för att hämta token utan certifikat (test):

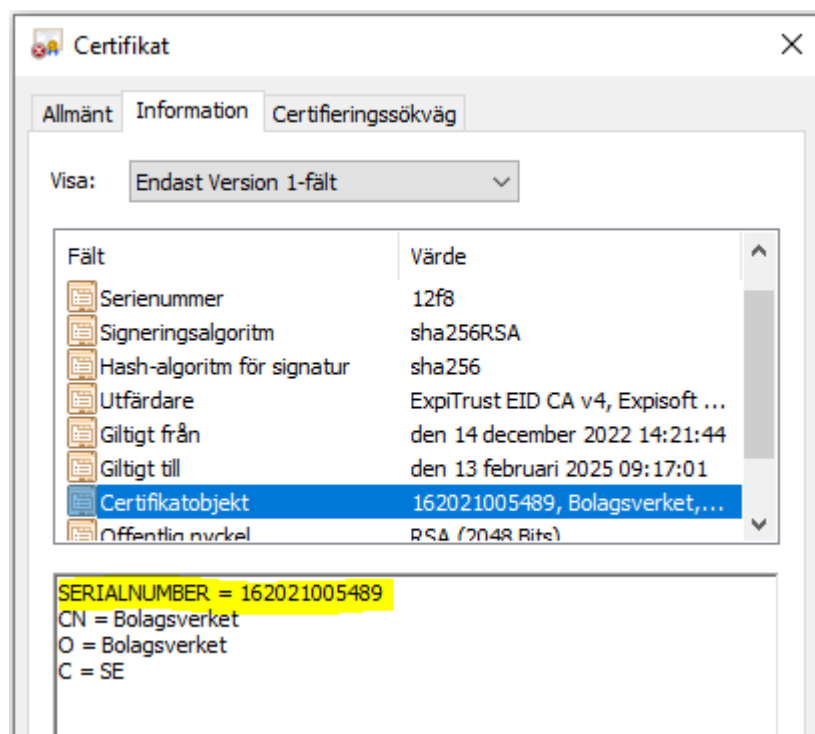
<https://portal-accept2.api.bolagsverket.se/oauth2/token>

5.1 Validering av klientcertifikat

Om man önskar nyttja ett klientcertifikat (även kallat organisationscertifikat) vid autentiseringen måste datakonsumenten konfigureras för "mutual TLS" och presentera organisationscertifikatet vid TLS-handskakningen. Certifikatet måste vara utfärdat av organisation Expisoft AB för test- eller produktion med något av nedanstående DN:

- CN=ExpiTrust EID CA v4,O=Expisoft AB,C=SE
- CN=ExpiTrust **Test** CA v8,O=Expisoft AB,C=SE (**fungerar endast i testmiljö "accept2"**)

Certifikatet ska innehålla ett "SERIALNUMBER" med datakonsumentens 10-siffriga organisationsnummer prefixat med 16 i certifikatets DN. Detta måste överensstämja med datakonsumentens organisationsnummer – exempelvis generella kommun-a-certifikat med test-organisationsnummer accepteras **inte**. Se exempel nedan som visar Bolagsverkets organisationscertifikat utfärdat av Expisoft:



Om datakonsumenten redan har integrationer med myndigheters tjänster, till exempel hos Skatteverket, är det sannolikt att datakonsumenten redan har ett organisationscertifikat utfärdat av Expisoft som går att använda även mot SSBTGO Notifiering. 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.

5.2 Generera access token från applikation

Ett typiskt flöde för att generera och nyttja en access token innebär följande:

1. Generera en access token genom att skicka ett http POST-anrop till https://sysorgauth.bolagsverket.se/auth/realms/sysorg/protocol/openid-connect/token?client_id=<client_id> (produktion). Anropet kräver en "basic authorization" header. Det vill säga en header vid namn "Authorization" med innehållet "Basic <credentials>" där "<credentials>" är en Base64-kodad sträng av "client id" och "secret id" konkatenerat med ett kolon. Därtill ska "grant_type" och "scope" anges i formulärsinnehållet som skickas. Se kapitel "Exempel" nedan.
2. Den access token man får tillbaka i svaret har en giltighetstid. Se värde för "expires_in" i JSON-svaret. Värdet anger hur många sekunder token är giltig.
3. Genomför anrop till API:et och skicka med en header vid namn "Authorization". Denna gång med innehåll "Bearer <credentials>" där "<credentials>" ersätts med access_token-värdet man fick tillbaka i svaret i steg 2.
4. När giltighetstiden är på väg att gå ut återgår man till steg 1 och genererar en ny token.

Om man vill återkalla en access token innan giltighetstiden gått ut så att den inte kan användas för ytterligare anrop kan ett http POST-anrop göras mot:

URL för att återkalla token utfärdad med klientcertifikat (produktion):

<https://sysorgauth.bolagsverket.se/auth/realms/sysorg/protocol/openid-connect/revoke>

URL för att återkalla token utfärdad med klientcertifikat (test): <https://sysorgauth-accept2.bolagsverket.se/auth/realms/sysorg/protocol/openid-connect/revoke>

URL för att återkalla token utfärdad utan certifikat (produktion):

<https://portal.api.bolagsverket.se/oauth2/revoke>

URL för att återkalla token utfärdad utan certifikat (test):

<https://portal-accept2.api.bolagsverket.se/oauth2/revoke>

Även detta anrop ska göras med "basic authorization" header, precis som i steg 1 ovan. Därtill ska token anges i formulärsinnehållet som skickas. Se kapitel "Exempel" nedan.

6 URL:er för API-resurser

Följande URL:er gäller för de resurser som API:et exponerar. Giltiga scopes är "ssbtgo-notifiering:ping" för "/isalive"-resursen och "ssbtgo-notifiering:read" eller "ssbtgo-notifiering:write" för övriga resurser, beroende på om man ska läsa eller skriva.

För att kontrollera om applikationen svarar skickas ett http GET-anrop till:

Produktion: <https://gw.api.bolagsverket.se/ssbtgo-notifiering/v1/isalive>

Test: <https://gw-accept2.api.bolagsverket.se/ssbtgo-notifiering/v1/isalive>

För att hämta alla services skickas ett http GET-anrop till:

Produktion: <https://gw.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant>

Test: <https://gw-accept2.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant>

För att konfigurera service för prenumeration skickas ett http POST-anrop till:

Produktion: <https://gw.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant>

Test: <https://gw-accept2.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant>

För att hämta konfiguration för en service skickas ett http GET-anrop till:

Produktion: <https://gw.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant/{service}>

Test: <https://gw-accept2.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant/{service}>

För att ta bort prenumerationer för en service skickas ett http DELETE-anrop till:

Produktion: <https://gw.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant/{service}>

Test: <https://gw-accept2.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant/{service}>

För att hämta lista på prenumerationer skickas ett http GET-anrop till:

Produktion: <https://gw.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant/{service}/prenumeration>

Test: <https://gw-accept2.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant/{service}/prenumeration>

För att skapa eller ta bort prenumerationer i batch skickas ett http POST-anrop till:

Produktion: <https://gw.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant/{service}/prenumeration>

Test: <https://gw-accept2.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant/{service}/prenumeration>

För att kontrollera om prenumeration finns för organisationsnummer skickas ett http GET-anrop till:

Produktion: <https://gw.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant/{service}/prenumeration/{orgnr}>

Test: <https://gw-accept2.api.bolagsverket.se/ssbtgo-notifiering/v1/prenumerant/{service}/prenumeration/{orgnr}>

7 Exempel

I våra exempel använder vi oss av cURL-anrop exporterade från verktyget "Insomnia". Notera att två olika exempelvärden används för "Basic <credentials>". Dessa är Base64-kodade strängar av "exempel_client_id:exempel_client_secret" och "mittKlientID:" vilket ger oss värdena "ZXh1bXB1bF9jbGllbnRfaWQ6ZXh1bXB1bF9jbGllbnRfc2VjcmV0" och "bWl0dEtMaWVudEIEOg==" där det förstnämnda värdet nyttjas i det vanliga client credentials-flödet och det andra för ett klientcertifikats-flöde. URL är satt till test.

7.1 Generera en access token (klientcertifikat)

Anrop mot testmiljö:

```
curl --request POST \  
  --url 'https://sysorgauth-accept2.bolagsverket.se/auth/realms/sysorg/protocol/openid-connect/token?client_id=mittKlientID' \  
  --header 'Authorization: Basic bWl0dEtMaWVudEIEOg==' \  
  --header 'Content-Type: application/x-www-form-urlencoded' \  
  --data grant_type=client_credentials \  
  --data 'scope=ssbtgo-notifiering:read ssbtgo-notifiering:ping'
```

Svar:

```
{  
  "access_token": "värdePåGenereradAccessToken",  
  "scope": "ssbtgo-notifiering:read",  
  "token_type": "Bearer",  
  "expires_in": 3600  
}
```

7.2 Generera en access token (utan certifikat)

Anrop mot testmiljö:

```
curl --request POST \  
  --url https://portal-accept2.api.bolagsverket.se/oauth2/token \  
  --header 'Authorization: Basic  
ZXh1bXB1bF9jbGllbnRfaWQ6ZXh1bXB1bF9jbGllbnRfc2VjcmV0' \  
  --header 'Content-Type: application/x-www-form-urlencoded' \  
  --data grant_type=client_credentials \  
  --data scope=ssbtgo-notifiering:read
```

Svar:

```
{  
  "access_token": "värdePåGenereradAccessToken",  
  "scope": "ssbtgo-notifiering:read",  
  "token_type": "Bearer",  
  "expires_in": 3600  
}
```

7.3 Återkalla en access token (utfärdad utan certifikat)

Anrop mot testmiljö:

```
curl --request POST \  
  --url https://portal-accept2.api.bolagsverket.se/oauth2/revoke \  
  --header 'Authorization: Basic \  
ZXhlcXBibF9jbGllbnRfaWQ6ZXhlcXBibF9jbGllbnRfc2VjcmV0' \  
  --header 'Content-Type: application/x-www-form-urlencoded' \  
  --data token=värdePåGenereradAccessToken
```

Svar:

```
HTTP-statuskod 200 returneras.
```

7.4 Anropa resurs "isalive"

Anrop mot testmiljö:

```
curl --request GET \  
  --url https://gw-accept2.api.bolagsverket.se/ssbtgo-notifiering/v1/isalive \  
  --header 'Authorization: Bearer värdePåGenereradAccessTokenMedScopePing' \  
  --header 'accept: */*'
```

Svar:

```
HTTP-statuskod 200 returneras.
```

7.5 Ytterligare exempel

För exempel på anrop mot övriga resurser se Swagger-specifikationen. Där kan man se vad som kan skickas med som JSON-data för POST-anropen mot de olika resurserna.