# Utkast 2021-05-19 Intygsväxling - OAuth2 token service

> Observera att informationen i detta dokument är arbetsmaterial och ska inte betraktas som fastställda eller gällande.
>
> Eftersom detta är en delmängd av handboken så finns det länkar som inte fungerar.



## Termer och begrepp

| Begrepp | Beskrivning |
|---|---|
| **Identitetsintyg** | Intyg som utfärdas av en identitetsintygsutfärdare efter autentisering och innehåller egenskaper kopplat till identitet samt kan innehålla andra personlig egenskaper även kallade behörighetsattribut. Intyget baseras på Security Assertion Markup Language (SAML). En standard baserat på XML för att överföra säkerhetsrelaterad information på ett strukturerat sätt, samt digitalt representera användaren och dess information. |
| **Identitetsintygsutfärdare** | Utfärdare av identitetsintyg innehållande identitets- och behörighethetsattribut för den användare som autentiserat sig. |
| **Åtkomstintyg** | Ett digitalt intyg som representerar användaren och ger denna åtkomst till bastjänster eller motsvarande. Kallas inom OAuth2 för access token. Kan även jämföras med ett SAML-intyg, skillnaden ligger huvudsakligen i det tekniska formatet.<br><br>OAuth 2.0 specifikation RFC 6749, Access token |
| **Förnyelseintyg** | Ett digitalt intyg som ställs ut till det aktörssystem som representerar användaren och dess åtkomster. Ger aktörssystemet möjlighet att skapa nya åtkomstintyg för användaren under dess giltighetstid.<br><br>OAuth 2.0 specifikation RFC 6749, Refresh token |
| **Client Identifier** | Begrepp inom Oauth2 för att identifiera aktörssystemet, unikt och används i kombination med client secret. |
| **Client Secret** | Lösenord eller hemlighet för att autentisera aktörssystemet. |
| **Revokering** | Att återkalla/avsluta ett giltigt och pågående intyg för åtkomst eller förnyelse. |
| **Introspection** | Funktionalitet att kunna fråga om status eller meta-data kopplat till ett utfärdat intyg. |

## Inledning

Intygsväxling från identitetsintyg till åtkomstintyg och tillhörande förnyelseintyg syftar i grunden på att skapa en lösare koppling mellan autentisering och auktorisation. Förnyelseintyget ger även möjlighet till längre sessioner genom att åtkomstintyget förnyas regelbundet, samtidigt som giltighetstiden för åtkomstintyget och identitetsintyget kan hållas kortare.

Den intygsväxling som E-hälsomyndigheten erbjuder utgår från RFC 7522 (*Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants*) och ger därmed möjlighet att växla från identitetsintyg enligt SAML 2.0 till åtkomst- och förnyelseintyg enligt OAuth 2.0.

Följande stödjs av tjänsten för intygsväxling eller användande av OAuth-åtkomstintyg:

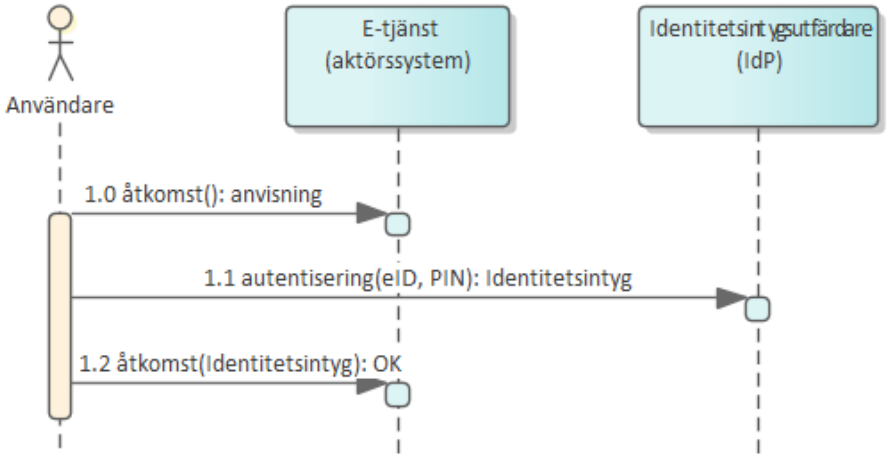
- Alla roller (vård, apotek samt privatperson) kan växla ett giltigt SAML-intyg till ett åtkomstintyg (access token) för vidare åtkomst
- Alla bastjänster från E-hälsomyndigheten kan anropas med en OAuth2 access token
- Åtkomstintyget har en giltighetstid på 60 minuter
- Via förnyelseintyget (refresh token) växla till sig ett nytt åtkomstintyg. (Se även Giltighetstid intyg)
- Skapa client-secret
- Byte av client-secret
- Stöd för flödet Assertion Flow/Implicit flow
- Åtkomstintyget (access token) som är av typen JSON Web Token (JWT), skyddas mot insyn med hjälp av JSON Web Encryption (JWE). Åtkomstintyget är därmed inte läsbart för annan part än E-hälsomyndigheten.
- HTTP Basic som autentiseringsmetod för klienter. [RFC 6749, 2.3.1]

Följande stödjs inte:

- Inget stöd för att invalidera eller avsluta ett giltigt åtkomstintyg innan dess giltighetstid är slut.
- Inget stöd för "prompt", det vill säga påkalla slutanvändarens uppmärksamhet.
- Inget stöd för introspection

# Anropsflöde

För att genomföra en intygsväxling behöver användaren vara autentiserad och ett giltigt identitetsintyg behöver vara utfärdad och tillgänglig för E-tjänsten att intygsväxla.




*Figur 1 - Förenklat exempel på ett autentisering- och auktorisationsflöde, utfärdande av identitetsintyg.*

1.0 Användaren begär åtkomst till E-tjänsten, eftersom användaren inte är autentiserad/auktoriserad så sker anvisning vald identitetsintygsutfärdare.

1.1 Användaren autentiserar sig mot identitetsintygsutfärdaren med sin personliga e-legitimation som sedan utfärdar ett identitetsintyg.

1.2 Användare begär åtkomst till E-tjänsten och bifogar identitetsintyget. Efter att E-tjänsten auktoriserat användaren ges åtkomst.

När E-tjänsten har ett identitetsintyg utfärdat för användaren kan intygsväxling ske, antigen genom direkt växling eller efter att ha kompletterat med behörighetsattribut.

- Intygsväxling med identitetsintyg
- Intygsväxling med identitetsintyg och kompletterande behörighetsattribut från E-tjänsten

Efter genomförd intygsväxling finns möjlighet att förnya åtkomstintyg genom att använda det förnyelseintyg som utfärdades som en del av den initiala växlingen från identitetsintyget. Efter att förnyelseintyget gått ut behöver ett nytt identitetsintyg utfärdas av identitetsintygsutfärdaren och en ny intygsväxling behöver genomföras.

- Åtkomstintyg genom förnyelse

Efter att intygsväxling eller förnyelse genomförts kan åtkomstintyget användas för åtkomst till E-hälsomyndighetens bastjänster.

- Anrop till bastjänst med åtkomstintyg

# Intygsväxling med identitetsintyg

Intygsväxling sker med identitetsintyg som utfärdats av identitetsintygsutfärdaren och innehåller användarens identitet och de behörighetsattribut som ligger till grund för den tänkta åtkomsten.


*Figur 2 - Intygsväxling med identitetsintyg*

1.0 E-tjänsten begär att växla in identitetsintyget och bifogar även användarnamn (client identifier) och lösenord (client secret).

1.1 Authorization Server returnerar ett åtkomstintyg (access token) ihop med ett förnyelseintyg (refresh token).

Om en klient väljer att använda sig av förnyelseintyg behöver klienten spara detta på ett säkert sätt i sin applikation. När klienten växlar sitt förnyelseintyg mot ett nytt åtkomstintyg returneras inget nytt förnyelseintyg, utan klienten förväntas använda det förnyelseintyg som returnerades i #2 vid varje förnyelse av åtkomstintyg.

## Parametrar som stöds

En mer detaljerad beskrivningen av respektive parameter återfinns i gränssnittsbeskrivningen.

| Inparameter | Beskrivning/värde |
|---|---|
| `grant_type` | `urn:ietf:params:oauth:grant-type:saml2-bearer` |
| `assertion` | Identitetsintyg |

I svar ges följande parametrar i en JSON-struktur:

| Utparameter | Beskrivning/värde |
|---|---|
| `access_token` | Åtkomstintyg |
| `expires_in` | Giltighetstid i sekunder på åtkomstintyget. |
| `token_type` | `bearer` |
| `refresh_token` | Förnyelseintyg |

## Exempel på anrop

**Fråga**

```
POST [host]/oauth2/api/oauth/token HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: application/x-www-form-urlencoded
Authorization: Basic RUhNLVVTRVI6RUhNLVBTVw==
Content-Length: 6819
Host: [host]:[port]
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.5.2 (Java/1.8.0_152)

grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Asaml2-
bearer&assertion=[SAML2:Assertion]
```

Exempel på svar:

**Svar**

```
{
"access_token" : "[access_token]",
"expires_in" : 3600,
"token_type" : "bearer",
"refresh_token" : "[refresh_token]"
}
```

## Intygsväxling med identitetsintyg och kompletterande behörighetsattribut från E-tjänsten

**OBS!**

I nuläget erbjuds endast kompletterande behörighetsattribut när Sweden Connect används som identitetsfederation. Aktiviteter pågår kring att se över möjligheterna att erbjuda motsvarande även med Sambi som identitetsfederation

Intygsväxling sker från identitetsintyget som innehåller användarens identitet och kan innehålla behörighetsattribut. E-tjänsten kompletterar sedan med behörighetsattribut på sidan av identitetsintyget som en del av intygsväxlingen. Se även "**Riktlinjer för tillhandahållare av behörighetsstyrande attribut**" för krav kopplat till E-tjänsten för att få tillhandahålla kompletterande behörighetsattribut.

Resultatet blir detsamma som om identitetsintyget skulle ha innehållet samtliga behörighetsattribut, det vill säga att det utfärdade åtkomstintyget innehåller kombinationen av de båda. I de fall som ett behörighetsattribut återfinns i både identitetsintyget och som kompletterande behörighetsattribut från E-tjänsten är det den från E-tjänsten som anses vara mer aktuell och därmed kommer att användas.

*Figur 3 - Intygsväxling med identitetsintyg och kompletterande behörighetsattribut från E-tjänsten.*

1.0 E-tjänsten paketerar och signerar relevanta behörighetsattribut enligt strukturen för parametern authorization_data.

1.1 E-tjänsten begär att växla in identitetsintyget och bifogar även användarnamn (client identifier), lösenord (client secret) och de kompletterande behörighetsattributen (authorization-data)

1.2 Authorisation Server returnerar ett åtkomstintyg (access token) ihop med ett förnyelseintyg (refresh token).

## Parametrar som stöds

En mer detaljerad beskrivningen av respektive parameter återfinns i gränssnittsbeskrivningen.

| Inparameter | Beskrivning/värde |
|---|---|
| `grant_type` | `urn:ietf:params:oauth:grant-type:saml2-bearer` |
| `assertion` | Identitetsintyg. |
| `authorization-data` | Kompletterande behörighetsattribut från E-tjänsten. Se länk för format. |

I svar ges följande parametrar i en JSON-struktur:

| Utparameter | Beskrivning/värde |
|---|---|
| `access_token` | Åtkomstintyg |
| `expires_in` | Giltighetstid i sekunder på åtkomstintyget |
| `token_type` | `bearer` |
| `refresh_token` | Förnyelseintyg |

## Exempel på anrop

Ett exempel på förmedling av behörighetsattribut för en farmaceut på ett öppenvårdsapotek. Formatet på exemplet är enligt JWT/JWS och tre delar. Där grön text motsvarar huvudet och blå själva meddelandet och den rosa den omslutande signeringen.

```
{
    "alg": "HS256",
    "typ": "JWT"
}
{
    "jti": "19a9d58c-d016-47c0-8ea9-a11a0812c85c",
    "iss": "e-tjanst-client-id",
    "iat": 1516239022,
    "pharmacyIdentifier": "1234567890123",
    "healthcareProfessionalLicenseIdentityNumber": "123456",
    "healthcareProfessionalLicense": "AP"
}

@HMACHS256( base64UrlEncode(header) + "." + base64UrlEncode(payload) , <client_secret> )
```

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJqdGkiOiIxOWE5ZDU4Yy1kMDE2LTQ3YzAtOGVhOS1hMTFhMDgxMmM4NWMiLCJpc3MiOiJlLXRqYW5zdC1jbGllbnQtaWQiLCJpYXQiOjE1MTYyMzkwMjIsInBoYXJtYWN5SWRlbnRpZmllciI6IjEyMzQ1Njc4OTAxMjMiLCJoZWFsdGhjYXJlUHJvZmVzc2lvbmFsTGljZW5zZUlkZW50aXR5TnVtYmVyIjoiMTIzNDU2IiwiaGVhbHRoY2FyZUByb2Zlc3Npb25hbExpY2Vuc2UiOiJBUCJ9.zhRRnduGLcm6nJ7zXrpdZjIEq7lELToaoYyVe9ZA3xk
```

Anropet till intygsväxlingen skulle då se ut enligt

```
POST [host]/oauth2/api/oauth/token HTTP/1.1

Accept-Encoding: gzip,deflate
Content-Type: application/x-www-form-urlencoded
Authorization: Basic RUhNLVVTRVI6RUhNLVBTVw==
Content-Length: 6819
Host: [host]:[port]
Connection: Keep-Alive
User-Agent: HttpClient

grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Asaml2-bearer&assertion=[Identitetsintyg]&auth
orization-data=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJqdGkiOiIxOWE5ZDU4Yy1kMDE2LTQ3YzAtOGVhOS1hMTF
hMDgxMmM4NWMiLCJpc3MiOiJlLXRqYW5zdC1jbGllbnQtaWQiLCJpYXQiOjE1MTYyMzkwMjIsInBoYXJtYWN5SWRlbnRpZmllci
I6IjEyMzQ1Njc4OTAxMjMiLCJoZWFsdGhjYXJlUHJvZmVzc2lvbmFsTGljZW5zZUlkZW50aXR5TnVtYmVyIjoiMTIzNDU2Iiwia
GVhbHRoY2FyZVByb2Zlc3Npb25hbExpY2Vuc2UiOiJBUCJ9.zhRRnduGLcm6nJ7zXrpdZjIEq7lELToaoYyVe9ZA3xk
```

# Åtkomstintyg genom förnyelse

Förnyelse av åtkomstintyget kan ske inom ramen för förnyelseintygets giltighetstid (Se Giltighetstid intyg). Förnyelse kan ske innan eller i samband med att ett befintligt åtkomstintyg är på väg att bli ogiltigt och påverkar inte befintliga åtkomstintyg, det vill säga det är möjligt att ha flera giltiga samtidigt.


*Figur 4 - Åtkomstintyg genom förnyelse*

1.0 E-tjänsten begär att förnya åtkomstintyget och bifogar användarnamn (client identifier), lösenord (client secret) och förnyelseintyget (refresh_token)

1.1 Authorisation Server returnerar ett nytt åtkomstintyg (access token).

## Parametrar som stöds

En mer detaljerad beskrivningen av respektive parameter återfinns i gränssnittsbeskrivningen.

| Inparameter | Beskrivning |
|---|---|
| `grant_type` | `refresh_token` |
| `refresh_token` | Förnyelseintyg |

I svar ges följande parametrar i en JSON-struktur:

| Utparameter | Beskrivning |
|---|---|
| `access_token` | Åtkomstintyg |
| `expires_in` | Giltighetstid på åtkomstintyget i sekunder. |

| | |
|---|---|
| token_type | bearer |

### Exempel på anrop

**Fråga**

```
POST [host]/oauth2/api/oauth/token HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: application/x-www-form-urlencoded
Authorization: Basic RUhNLVVTRVI6RUhNLVBTVw==
Content-Length: 916
Host: [host]
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.5.2 (Java/12.0.1)

grant_type=refresh_token&refresh_token=[Förnyelseintyg]
```

**Svar**

```
{
"access_token" : "[Åtkomstintyg]",
"expires_in" : 3600,
"token_type" : "bearer"
}
```

# Gränssnittsspecifikation

## Meddelandehuvud

| Headerparameter | Beskrivning |
|---|---|
| Authorization | För att anropa OAuth2 tokenservice krävs autentiseringsuppgifter som erhålls från E-hälsomyndighetens Servicedesk. E-hälsomyndigheten skapar client och secret som tilldelas en specifik aktör. Detta lösenord används av aktörssystemen som identifiering vid all intygsväxling. Vid anrop ska anges detta lösenord anges i format Base64 encoding enligt HTTP Basic Access Authentication (RFC 7617). Exempel:<br>`Authorization: Basic RUhNLVVTRVI6RUhNLVBTVw==` |
| Content-Type | Anges som "application/x-www-form-urlencoded"<br>`Content-Type: application/x-www-form-urlencoded` |

## In- och utparametrar

Vid intygsväxling anges följande parametrar i HTTP-body (enligt format application/x-www-form-urlencoded):

| Inparameter | Beskrivning |
|---|---|
| `grant_type` | Anges med värde “urn:ietf:params:oauth:grant-type:saml2-bearer“ då identitetsintyg används<br><br>Anges med värde "refresh_token" då förnyelseintyget används |
| `assertion` | Anges som Base64 encodat SAML2:Assertion alternativt det förnyelseintyg som utfärdats. |
| `authorization_data` | Används enbart då kompletterande behörighetsattribut anges. En JWT-token enligt länk. |

I svar ges följande parametrar i en JSON-struktur:

| Utparameter | Beskrivning |
|---|---|
| `access_token` | Krypterat access_token i format JSON Web Token. som endast kan läsas av eHälsomyndighetens API-SP (Resource Server). Kan användas vid anrop till E-hälsomyndighetens tjänster. Se |
| `expires_in` | Giltighetstid på det returnerade access-token i sekunder från det att det genererades. Idag 3600 sekunder (60 minuter) |
| `token_type` | Anges som "bearer" |
| `refresh_token` | En refresh_token i format JSON Web Token. kommer att returneras vid intygsväxling med SAML-intyg. Denna refresh_token är giltig i 420 minuter (7 timmar) |

## Authorization_data

För att komplettera med behörighetsattribut från E-tjänst förmedlas dessa enligt formatet JSON Web Token (JWT) och signeras i enlighet med JSON Web Signature (JWS).

| Reserverade claim eller header parametrar som ska ingå. | Beskrivning | Värde |
|---|---|---|
| `typ` | Identifierar formatet och sätts till JWT enligt standarden. | `JWT` |
| `alg` | Vald algoritm för signering av intyget. | `HS256` |
| `jti` | Unik identifierar för intyget. Används huvudsakligen för spårbarhet. | `UUID` |
| `iss` | Identifierar den utfärdande E-tjänst och sätts till den client identifier som tilldelats för intygsväxling. | `<client_id>` |
| `iat` | Tidpunkt för utfärdandet av intyget med behörighetsattributen. | `<tidpunkt, numeriskt värde>` |

Attribut/claims som förmedlas ska följa namnsättningen från Behörighetsstyrning med anpassningen att den fulla namnrymden inte tas med, utan endast namnet på attributet. Exempelvis skulle attributet *http://sambi.se/attributes/1/pharmacyIdentifier* anges med den kortare formen *pharmacyIdentifier.*