OAuch Compliance Report

This report contains the results of an automated security compliance assessment of the OAuth 2.0 implementation hosted on the server **test.musicbrainz.org**

https://distrinet.cs.kuleuven.be/
Contact: info@oauch.io

Introduction

OAuch is a security best practices and threats analyzer for OAuth 2.0 authorization server implementations. Its main goal is to analyze the compliance of an authorization server with the OAuth standards to uncover unmitigated threats and point out security improvements. OAuch tests an authorization server using a large set of test cases to check an authorization server's compliance with the security specifications defined in the original OAuth 2.0 standard, as well as other documents that refine the security assumptions and requirements. These documents include the OAuth threat model, the Security Best Current Practices, and others. In addition to OAuth, OAuch also supports OpenID Connect providers.

OAuch generates a comprehensive report of the analyzed authorization server that lists all the countermeasures that the authorization server does or does not support, as well as any deprecated features that are enabled. These results are then fed into a threat analysis process where all threats that apply to OAuth implementations are evaluated. For each threat, the analysis determines whether the threat is fully mitigated, partially mitigated, or unmitigated. OAuch also informs the user how to further mitigate threats that are not yet fully mitigated.

OAuch focuses on the authorization server recommendations and thus only tests the behavior of an authorization server implementation. Security issues on the authorization server side typically have a higher impact than issues on the OAuth client side. Some OAuth-related threats can be mitigated on the client. However, in the threat analysis, OAuch considers a worst-case scenario and assumes that a client does not have these mitigations in place. This is not an unlikely assumption: it has been shown in the academic literature that many clients have a flawed implementation and are unsafe. Threats that can only be mitigated on the client and not on the server are not considered.

This document provides a summary of the analysis. It also contains a list of all the problems or missing countermeasures that have been found in the tested implementation.

Site Rating and Scores

OAuch calculates several statistics after each test run. The most important output is the number of unmitigated threats. These threats represent weak points in the implementation, which can be exploited under the right circumstances. The number of partially mitigated threats and deprecated features are the second most important outputs. Partially mitigated threats may or may not be exploitable; OAuch does not report to what degree these threats have been mitigated, only that there is at least one partial countermeasure active. Deprecated features should be avoided if possible, as they are typically deprecated on the grounds of being insecure.

In addition to these three important indicators, OAuch also computes the failure rates of the test cases. This metric is calculated by dividing the number of failed tests by the total number of tests that are executed and converting the result to a percentage. This percentage indicates to what degree an authorization server correctly implements the OAuth specification. An overall failure rate is reported, as well as the individual failure rates of the three requirement levels that are used in the OAuth specification (*must*, *should*, *may*). The calculation only takes executed tests into account. Tests that are skipped because they are not relevant for the authorization server do not affect the result.

A test run will execute more test cases if the authorization server supports many flows or enables more features. This will increase the number of failed test cases, but will also increase the number of executed tests, keeping the failure rate relatively stable.

To enable users to quickly interpret the results of an analysis, OAuch uses the number of unmitigated threats to calculate a simple A/B/C rating for a site. Sites with zero or one unmitigated threat(s) are assigned an **A** rating, sites with 5 or less unmitigated threats a **B** rating, and sites with more unmitigated threats a **C** rating. This rating is designed to give an immediate impression of how well the tested site is doing.

Summary of the results

- **Test ID:** `5957ef4d-1cc6-46a6-b48a-7fda77fb7de7`
- **Test date:** april 24, 2024
- **Site name:** MetaBrainz OAuth (`e39ddd5c-9134-41aa-acb6-2416ce76f641`)

The site has been tested for compliance with the security requirements in the following OAuth and/or OpenID Connect specification(s):

- *The OAuth 2.0 Authorization Framework* (**RFC6749**)
- *The OAuth 2.0 Authorization Framework: Bearer Token Usage* (**RFC6750**)
- *Proof Key for Code Exchange by OAuth Public Clients* (**RFC7636**)
- *OAuth 2.0 Threat Model and Security Considerations* (**RFC6819**)
- *OAuth 2.0 Token Revocation* (**RFC7009**)
- *OAuth 2.0 Security Best Current Practice* (**SecBCP**)

Out of a total of 93 tests that were selected for this site, 74 tests succeeded and 19 tests failed (failure rate: 20,4%). Another 4 test(s) were skipped because they were not relevant for this site's configuration or because they were excluded.

OAuch has tested the following OAuth flows:

- **Implicit grant (response type 'token')** (access tokens)
- **Authorization Code grant** (access tokens; refresh tokens)

Any other OAuth flows were either not working or were configured to be excluded from the test process.

A+

Threats

- Mitigated threats: **29**
- Partially mitigated threats: **3**
- Unmitigated threats: **0**

Deprecated features

- Deprecated features detected: **2**

Countermeasures

- Mandatory test cases failed: **3** (6,2%)
- Recommended test cases failed: **3** (21,4%)
- Optional test cases failed: **2** (28,6%)
- Overall test cases failed: **8** (11,6%)

Document	Mandatory	Recommended	Optional
RFC6749	**2** (6%)	-	**1** (33%)
RFC6750	-	-	-
RFC7636	-	-	**1** (100%)
RFC6819	-	-	-
RFC7009	**1** (20%)	-	**1** (100%)
SecBCP	-	**3** (43%)	-

Table 1: *A per-document overview of the failed test cases, grouped by requirement level.*

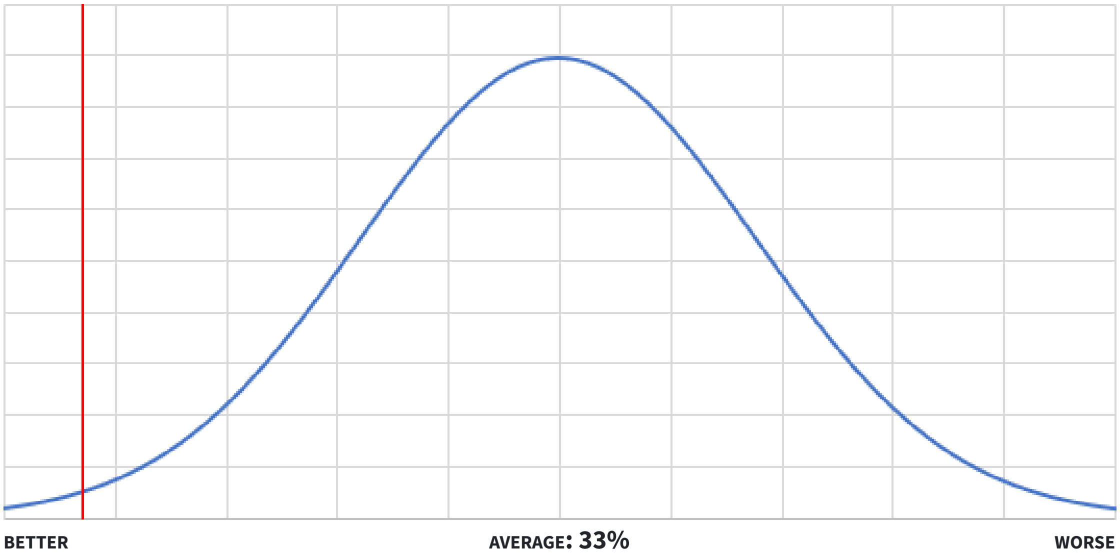

Figure 1: *The distribution of failure rates for other tested sites. The position of your site is indicated with the red vertical line. This distribution is based on an ecosystem analysis performed on 100 sites in December 2020. More information on* [*https://lirias.kuleuven.be/3765111?limo=0*]

Threats

The OAuth working group has published a comprehensive threat model shortly after publishing the original OAuth 2.0 standard. This threat model is further refined in the latest Security Best Current Practices document to include additional threats that have been observed in real-world usage of OAuth. The threat model describes for each threat how an implementation may be attacked and which countermeasures can be applied. Some threats are mitigated by a combination of multiple countermeasures, while others can be mitigated by a single countermeasure. In many cases, alternative sets of countermeasures may be used to address a threat. Some countermeasures may (partially) mitigate multiple threats. The model assumes a powerful attacker that has full access to the network between the OAuth client and the authorization server, and the client and the resource server. The attacker may eavesdrop on any communication between those parties and has unlimited resources to mount attacks. In addition, two of the three parties involved in the OAuth protocol may collude to mount an attack against the 3rd party.

This threat model has been adopted in OAuch and is used to offer precise feedback. OAuch uses test cases to detect which countermeasures are implemented by the authorization server. It then uses the information from the threat model to determine which threats are mitigated. For every threat, it takes the list of mitigations that are proposed by the threat model and compares it with the mitigations that have been detected. If the threat is properly mitigated, it is marked as fully mitigated. When no relevant countermeasures are active, the threat is unmitigated. Threats can also be partially mitigated if some countermeasures are present, but not all. When multiple sets of countermeasures can mitigate a threat, it is sufficient that only one set is fully implemented.

Threat "Authorization Code Injection"

In an authorization code injection attack, the attacker attempts to inject a stolen authorization code into the attacker's own session with the client. The aim is to associate the attacker's session at the client with the victim's resources or identity.

Threat status: **PARTIALLY MITIGATED**

This threat can be mitigated if all of the following countermeasures are fully implemented:

- Pkce.IsPkceImplemented [supported]
- Pkce.HashedPkceDisabled [supported]
- Pkce.IsPkceRequired [**not supported**]

Threat "Abuse of revoked tokens"

Leaked (and potentially long-lived) access or refesh tokens that cannot be revoked may enable an attacker to impersonate a user.

Threat status: **PARTIALLY MITIGATED**

This threat can be mitigated if all of the following countermeasures are fully implemented:

- Revocation.AccessRevokesRefresh [**not supported**]
- Revocation.CanAccessTokensBeRevoked [supported]
- Revocation.CanRefreshTokensBeRevoked [supported]
- Revocation.RefreshRevokesAccess [supported]

Threat "Unauthorized revocation of tokens"

An authentication server that supports token revocation must verify the ownership of a token before revocation.

Threat status: **PARTIALLY MITIGATED**

This threat can be mitigated if all of the following countermeasures are fully implemented:

- Revocation.IsBoundToClient [**not supported**]
- Revocation.IsClientAuthRequired [supported]

Deprecated Features

This section gives an overview of the features that are enabled on the tested site, but have been deprecated in newer specifications. Deprecated features may be enabled for backward compatibility reasons. However, features are typically deprecated because of security concerns. Hence, a careful analysis of the drawbacks must be made before enabling such a feature.

- Does the server support plain PKCE: **YES**
  This has been deprecated by RFC7636 and *SHOULD NOT* be used anymore.
- Is the implicit grant (response type = 'token') supported: **YES**
  This has been deprecated by the *Security Best Current Practices* document and *SHOULD NOT* be used anymore.

Test Settings

This section contains the settings that were used to run the test case. Note that these settings contain sensitive information such as the client secret. It is recommended to deactivate these values and revoke the appropriate permissions before distributing this document.

Basic Settings

- **Authorization URI**
  `https://test.musicbrainz.org/new-oauth2/authorize`
- **Callback URI**
  `https://oauch.io/Callback`
- **Token URI**
  `https://test.musicbrainz.org/new-oauth2/token`
- **Device Authorization URI**
  (empty)
- **Revocation URI**
  `https://test.musicbrainz.org/new-oauth2/revoke`

Client Identification

- **Client ID**
  `Bgc8hX3ZVAywDTsHPQ4oCn6k`
- **Client Secret**
  `QaQDNW67m9h8RjncUrizo4WrlrKF3UdbG1Kv5bTI2G10CRyq`
- **Client Certificate**
  no
- **Scope**
  `profile tag`
- **Alternative Client ID**
  `6uZuDUziHgYFFk4Orp6tbDUB`
- **Alternative Client Secret**
  `kczVgmpyAY3F3KjXB3wfuilNbIQb1cs6XiomVBh5rdHkqEx0`
- **Scope**
  `rating tag`

Grant-Specific Overrides

There are no grant-specific overrides.

API Settings

- **API Test URI**
  `https://test.musicbrainz.org/new-oauth2/userinfo`
- **HTTP Method**
  Get
- **Additional HTTP Headers**
  (empty)
- **Form POST Data**
  (empty)

OpenID Connect

- **Issuer**
  (empty)
- **JWKS URI**
  (empty)

Advanced Settings

- **Token Request Delay**
  0 seconds
- **Default PKCE Behavior**
  `None`
- **Response Mode**
  `Default`
- **Use a Request Parameter**
  No
- **Client Signing Key**
  (empty)
- **Client Authentication Mechanism**
  `ClientSecretPost`
- **Client Authentication Audience**
  (empty)

Test Results

The remainder of this document contains the description of the test cases that have failed and a detailed log of the test run. Test cases that succeeded are not included in this document. The results and logs of these omitted test cases can be found on the OAuch website.

Note that these logs contain sensitive information such as the client secret. It is recommended to deactivate these values and revoke the appropriate permissions before distributing this document.

TC1 - *AuthEndpoint.SupportsPostAuthorizationRequestsTest*

This test checks whether the authorization server supports sending authentication parameters via a POST request.

Requirement Level(s)

- RFC6749: **May**

Test result

- Does the server support POST authentication requests: **NO**
- Test status: **FAILED**

Test log

Test `AuthEndpoint.SupportsPostAuthorizationRequestsTest' started

ℹ Requesting a token via the Implicit grant (response type 'token')

◆ Redirecting pop-up

The pop-up window is being redirected to `/Callback/PostRedirect/5957ef4d1cc646a6b48a7fda77fb7de7?values=cmVzcG9uc2VfdHlwZT10b2tlbiZjbGllbnRfaWQ9QmdjOGhYM1pWQXl3RFRzSFBRNG9DbjZrJnJlZGlyZWN0X3VyaT1odHRwcyUzYSUyZiUyZm9hdWNoLmlvJTJmQ2FsbGJhY2smc3RhdGU9b2F1Y2hfc3RhdGVfdmFyJnNjb3BlPXByb2ZpbGUrdGFn`

ℹ User clicked the 'stalled test' button

ℹ No access tokens or identity tokens have been received from the server.

✕ Test 'AuthEndpoint.SupportsPostAuthorizationRequestsTest' was executed and failed.

Test `AuthEndpoint.SupportsPostAuthorizationRequestsTest' finished

TC2 - *AuthEndpoint.SameParameterTwiceDisallowedTest*

This test checks whether the authorization server accepts authorization requests with parameters that are included more than once.

Requirement Level(s)

- RFC6749: **Must**

Test result

- Does the authorization server allow multiple instances of the same parameter: **YES**
- Test status: **FAILED**

Test log

Test `AuthEndpoint.SameParameterTwiceDisallowedTest' started

Requesting a token via the Implicit grant (response type 'token')

Redirecting pop-up

The pop-up window is being redirected to `https://test.musicbrainz.org:443/new-oauth2/authorize?response_type=token&client_id=Bgc8hX3ZVAywDTsHPQ4oCn6k&redirect_uri=https%3a%2f%2foauch.io%2fCallback&state=oauch_state_var&scope=profile+tag&response_type=token`

Callback received

A callback was received from the OAuth provider at the URL `https://oauch.io/Callback#token_type=Bearer&access_token=mebo_iTgFATlQJjxBCr6nFE1D3tFLyg1enxUu6ecVHW04zk&expires_in=3600&state=oauch_state_var`

The request did not contain POST parameters.

Token result

```
{
  "AccessTokens": [
    "mebo_iTgFATlQJjxBCr6nFE1D3tFLyg1enxUu6ecVHW04zk"
  ],
  "IdentityTokens": []
}
```

Test 'AuthEndpoint.SameParameterTwiceDisallowedTest' was executed and failed.

Test `AuthEndpoint.SameParameterTwiceDisallowedTest' finished

TC3 - *TokenEndpoint.SameParameterTwiceDisallowedTest*

This test checks whether the token endpoint accepts authorization requests with parameters that are included more than once.

Requirement Level(s)

- RFC6749: **Must**

Test result

- Does the token endpoint allow multiple instances of the same parameter: **YES**
- Test status: **FAILED**

Test log

Test `TokenEndpoint.SameParameterTwiceDisallowedTest' started

Requesting a token via the Authorization Code grant

Redirecting pop-up

The pop-up window is being redirected to `https://test.musicbrainz.org:443/new-oauth2/authorize?response_type=code&client_id=Bgc8hX3ZVAywDTsHPQ4oCn6k&redirect_uri=https%3a%2f%2foauch.io%2fCallback&state=oauch_state_var&scope=profile+tag`

Callback received

A callback was received from the OAuth provider at the URL `https://oauch.io/Callback?code=l4SjQjA6D17hUroGdNicRPNJumFWOk0dKrDOpAXnYJDRBrYf&state=oauch_state_var#_`

The request did not contain POST parameters.

HTTP POST https://test.musicbrainz.org/new-oauth2/token

```
POST https://test.musicbrainz.org/new-oauth2/token
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 280

grant_type=authorization_code&code=l4SjQjA6D17hUroGdNicRPNJumFWOk0dKrDOpAXnYJDRBrYf&state=oauch_state_v
ar&redirect_uri=https%3a%2f%2foauch.io%2fCallback&client_id=Bgc8hX3ZVAywDTsHPQ4oCn6k&client_secret=QaQD
NW67m9h8RjncUrizo4WrlrKF3UdbG1Kv5bTI2G10CRyq&grant_type=authorization_code
```

HTTP 200 OK

```
HTTP 200 OK
Server: openresty
Date: Wed, 24 Apr 2024 20:22:30 GMT
Connection: keep-alive
Keep-Alive: timeout=15
Cache-Control: no-store
Pragma: no-cache
```

```
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Max-Age: 21600
X-Frame-Options: DENY
Content-Security-Policy: default-src 'self'; frame-ancestors 'none'; script-src 'sha256-vJFm4HtSvYBaeJG
b0uUgH6hZ77q54fbWtplmtKmB+RE=' https://fonts.gstatic.com https://test.musicbrainz.org;
Referrer-Policy: no-referrer
Vary: Cookie
Content-Type: application/json
Content-Length: 185

{"access_token": "mebo_iUQAYv9ZhPLqVspgsRQgW54v5WgXWFDOrRwKOiKiVJ", "expires_in": 3600, "refresh_toke
n": "mebr_HKF9Sf74X3igqIQUtn828BJH7LmVu9DuoQ02RliYGE6y6XSd", "token_type": "Bearer"}
```

● Token result

```
{
  "AuthorizationCode": "l4SjQjA6D17hUroGdNicRPNJumFWOk0dKrDOpAXnYJDRBrYf",
  "RefreshToken": "mebr_HKF9Sf74X3igqIQUtn828BJH7LmVu9DuoQ02RliYGE6y6XSd",
  "AccessTokens": [
    "mebo_iUQAYv9ZhPLqVspgsRQgW54v5WgXWFDOrRwKOiKiVJ"
  ],
  "IdentityTokens": []
}
```

✖ Test 'TokenEndpoint.SameParameterTwiceDisallowedTest' was executed and failed.

Test `TokenEndpoint.SameParameterTwiceDisallowedTest' finished

TC4 - *Pkce.IsPkceRequiredTest*

This test determines whether the server requires the use of PKCE for the authorization code grant.

Requirement Level(s)

- RFC7636: **May**
- SecBCP: **Should**

Test result

- Does the server require PKCE: **NO**
- Test status: **FAILED**

Test log

```
Test `Pkce.IsPkceRequiredTest' started

  ℹ   The server supports the authorization code grant without PKCE

  ✕   Test 'Pkce.IsPkceRequiredTest' was executed and failed.

Test `Pkce.IsPkceRequiredTest' finished
```

TC5 - *Revocation.IsBoundToClientTest*

This test checks if the revocation endpoint only revokes tokens that are bound to the authenticated client.

Requirement Level(s)

- RFC7009: **Must**

Test result

- Is revocation bound to a specific client: **NO**
- Test status: **FAILED**

Test log

Test `Revocation.IsBoundToClientTest' started

Requesting a token via the Authorization Code grant

Redirecting pop-up

The pop-up window is being redirected to `https://test.musicbrainz.org:443/new-oauth2/authorize?response_type=code&client_id=Bgc8hX3ZVAywDTsHPQ4oCn6k&redirect_uri=https%3a%2f%2foauch.io%2fCallback&state=oauch_state_var&scope=profile+tag`

Callback received

A callback was received from the OAuth provider at the URL `https://oauch.io/Callback?code=zyInBdYmcrgznSzKdlgTKJGWA1JAaVPrkixPSwo7wekiRbcv&state=oauch_state_var#_`

The request did not contain POST parameters.

HTTP POST https://test.musicbrainz.org/new-oauth2/token

```
POST https://test.musicbrainz.org/new-oauth2/token
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 250

grant_type=authorization_code&code=zyInBdYmcrgznSzKdlgTKJGWA1JAaVPrkixPSwo7wekiRbcv&state=oauch_state_v
ar&redirect_uri=https%3a%2f%2foauch.io%2fCallback&client_id=Bgc8hX3ZVAywDTsHPQ4oCn6k&client_secret=QaQD
NW67m9h8RjncUrizo4WrlrKF3UdbG1Kv5bTI2G10CRyq
```

HTTP 200 OK

```
HTTP 200 OK
Server: openresty
Date: Wed, 24 Apr 2024 20:24:01 GMT
Connection: keep-alive
Keep-Alive: timeout=15
Cache-Control: no-store
Pragma: no-cache
```

```
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Max-Age: 21600
X-Frame-Options: DENY
Content-Security-Policy: default-src 'self'; frame-ancestors 'none'; script-src 'sha256-vJFm4HtSvYBaeJG
b0uUgH6hZ77q54fbWtplmtKmB+RE=' https://fonts.gstatic.com https://test.musicbrainz.org;
Referrer-Policy: no-referrer
Vary: Cookie
Content-Type: application/json
Content-Length: 185

{"access_token": "mebo_PgdlbYlUFmk6JAF1nhhcttrToewXLmhIyK1L1Jvbgj", "expires_in": 3600, "refresh_toke
n": "mebr_4y0TlK4f6ssMTvWUKZoxOaa4eOCXTkySDrebWzwY96yfNEfo", "token_type": "Bearer"}
```

Token result

```
{
  "AuthorizationCode": "zyInBdYmcrgznSzKdlgTKJGWA1JAaVPrkixPSwo7wekiRbcv",
  "RefreshToken": "mebr_4y0TlK4f6ssMTvWUKZoxOaa4eOCXTkySDrebWzwY96yfNEfo",
  "AccessTokens": [
    "mebo_PgdlbYlUFmk6JAF1nhhcttrToewXLmhIyK1L1Jvbgj"
  ],
  "IdentityTokens": []
}
```

Revoking a refresh token

HTTP POST https://test.musicbrainz.org/new-oauth2/revoke

```
POST https://test.musicbrainz.org/new-oauth2/revoke
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 187

token=mebr_4y0TlK4f6ssMTvWUKZoxOaa4eOCXTkySDrebWzwY96yfNEfo&token_type_hint=refresh_token&client_id=6uZ
uDUziHgYFFk4Orp6tbDUB&client_secret=kczVgmpyAY3F3KjXB3wfuilNbIQb1cs6XiomVBh5rdHkqEx0
```

HTTP 200 OK

```
HTTP 200 OK
Server: openresty
Date: Wed, 24 Apr 2024 20:24:01 GMT
Connection: keep-alive
Keep-Alive: timeout=15
Cache-Control: no-store
Pragma: no-cache
X-Frame-Options: DENY
Content-Security-Policy: default-src 'self'; frame-ancestors 'none'; script-src 'sha256-vJFm4HtSvYBaeJG
b0uUgH6hZ77q54fbWtplmtKmB+RE=' https://fonts.gstatic.com https://test.musicbrainz.org;
Referrer-Policy: no-referrer
Vary: Cookie
Content-Type: application/json
Content-Length: 2

{}
```

The server accepted the revocation request with the wrong client id

× Test 'Revocation.IsBoundToClientTest' was executed and failed.

Test ` Revocation.IsBoundToClientTest' finished

TC6 - *Revocation.AccessRevokesRefreshTest*

This test checks whether the authorization server revokes refresh tokens after an access token from the same authorization grant is revoked.

Requirement Level(s)

- RFC7009: **May**

Test result

- Are refresh tokens revoked after access token revocation: **NO**
- Test status: **FAILED**

Test log

Test `Revocation.AccessRevokesRefreshTest' started

Requesting a token via the Authorization Code grant

Redirecting pop-up

The pop-up window is being redirected to `https://test.musicbrainz.org:443/new-oauth2/authorize?response_type=code&client_id=Bgc8hX3ZVAywDTsHPQ4oCn6k&redirect_uri=https%3a%2f%2foauch.io%2fCallback&state=oauch_state_var&scope=profile+tag`

Callback received

A callback was received from the OAuth provider at the URL `https://oauch.io/Callback?code=ZsJeoqFr8eNYJ1LbCehRvhdmrVKIIZk5zopnLGByNAkYSs46&state=oauch_state_var#_`

The request did not contain POST parameters.

HTTP POST https://test.musicbrainz.org/new-oauth2/token

```
POST https://test.musicbrainz.org/new-oauth2/token
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 250

grant_type=authorization_code&code=ZsJeoqFr8eNYJ1LbCehRvhdmrVKIIZk5zopnLGByNAkYSs46&state=oauch_state_v
ar&redirect_uri=https%3a%2f%2foauch.io%2fCallback&client_id=Bgc8hX3ZVAywDTsHPQ4oCn6k&client_secret=QaQD
NW67m9h8RjncUrizo4WrlrKF3UdbG1Kv5bTI2G10CRyq
```

HTTP 200 OK

```
HTTP 200 OK
Server: openresty
Date: Wed, 24 Apr 2024 20:24:03 GMT
Connection: keep-alive
Keep-Alive: timeout=15
Cache-Control: no-store
Pragma: no-cache
```

```
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Max-Age: 21600
X-Frame-Options: DENY
Content-Security-Policy: default-src 'self'; frame-ancestors 'none'; script-src 'sha256-vJFm4HtSvYBaeJG
b0uUgH6hZ77q54fbWtplmtKmB+RE=' https://fonts.gstatic.com https://test.musicbrainz.org;
Referrer-Policy: no-referrer
Vary: Cookie
Content-Type: application/json
Content-Length: 185

{"access_token": "mebo_qoHZes0DKDnLl4j4lXOnyBRDshSHAxt3TUkEuH7run", "expires_in": 3600, "refresh_toke
n": "mebr_5jbv8OdCnjXMydmblVwpCHUZYyogrL5ONiRVgXe1nmJPi6DE", "token_type": "Bearer"}
```

Token result

```
{
  "AuthorizationCode": "ZsJeoqFr8eNYJ1LbCehRvhdmrVKIIZk5zopnLGByNAkYSs46",
  "RefreshToken": "mebr_5jbv8OdCnjXMydmblVwpCHUZYyogrL5ONiRVgXe1nmJPi6DE",
  "AccessTokens": [
    "mebo_qoHZes0DKDnLl4j4lXOnyBRDshSHAxt3TUkEuH7run"
  ],
  "IdentityTokens": []
}
```

Revoking the access token...

Revoking an access token

HTTP POST https://test.musicbrainz.org/new-oauth2/revoke

```
POST https://test.musicbrainz.org/new-oauth2/revoke
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 180

token=mebo_qoHZes0DKDnLl4j4lXOnyBRDshSHAxt3TUkEuH7run&token_type_hint=access_token&client_id=Bgc8hX3ZVA
ywDTsHPQ4oCn6k&client_secret=QaQDNW67m9h8RjncUrizo4WrlrKF3UdbG1Kv5bTI2G10CRyq
```

HTTP 200 OK

```
HTTP 200 OK
Server: openresty
Date: Wed, 24 Apr 2024 20:24:04 GMT
Connection: keep-alive
Keep-Alive: timeout=15
Cache-Control: no-store
Pragma: no-cache
X-Frame-Options: DENY
Content-Security-Policy: default-src 'self'; frame-ancestors 'none'; script-src 'sha256-vJFm4HtSvYBaeJG
b0uUgH6hZ77q54fbWtplmtKmB+RE=' https://fonts.gstatic.com https://test.musicbrainz.org;
Referrer-Policy: no-referrer
Vary: Cookie
Content-Type: application/json
Content-Length: 2

{}
```

Waiting 5 seconds...

Refreshing a token

HTTP POST https://test.musicbrainz.org/new-oauth2/token

```
POST https://test.musicbrainz.org/new-oauth2/token
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 190

grant_type=refresh_token&refresh_token=mebr_5jbv8OdCnjXMydmblVwpCHUZYyogrL5ONiRVgXe1nmJPi6DE&client_id=
Bgc8hX3ZVAywDTsHPQ4oCn6k&client_secret=QaQDNW67m9h8RjncUrizo4WrlrKF3UdbG1Kv5bTI2G10CRyq
```

HTTP 200 OK

```
HTTP 200 OK
Server: openresty
Date: Wed, 24 Apr 2024 20:24:09 GMT
Connection: keep-alive
Keep-Alive: timeout=15
Cache-Control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Max-Age: 21600
X-Frame-Options: DENY
Content-Security-Policy: default-src 'self'; frame-ancestors 'none'; script-src 'sha256-vJFm4HtSvYBaeJG
b0uUgH6hZ77q54fbWtplmtKmB+RE=' https://fonts.gstatic.com https://test.musicbrainz.org;
Referrer-Policy: no-referrer
Vary: Cookie
Content-Type: application/json
Content-Length: 185

{"access_token": "mebo_CL54lEvfR2soCYougCMWO9RiyieP05xtV07Oyps6tQ", "expires_in": 3600, "refresh_toke
n": "mebr_lgMOPL0KnLHq3utLRF2ODcwajU0LbKvmeIeiYHc5GntDUqZK", "token_type": "Bearer"}
```

Token result

```
{
  "RefreshToken": "mebr_lgMOPL0KnLHq3utLRF2ODcwajU0LbKvmeIeiYHc5GntDUqZK",
  "AccessTokens": [
    "mebo_CL54lEvfR2soCYougCMWO9RiyieP05xtV07Oyps6tQ"
  ],
  "IdentityTokens": []
}
```

The refresh token has not been revoked

Test 'Revocation.AccessRevokesRefreshTest' was executed and failed.

Test `Revocation.AccessRevokesRefreshTest' finished

TC7 - *DocumentSupport.RFC8705SupportedTest*

This test determines whether the server supports RFC8705 'OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens'.

Requirement Level(s)

- SecBCP: **Should**

Test result

- Does the server support RFC8705 (mTLS): **NO**
- Test status: **FAILED**

Test log

```
Test `DocumentSupport.RFC8705SupportedTest' started

  ✖   Test 'DocumentSupport.RFC8705SupportedTest' was executed and failed.

Test `DocumentSupport.RFC8705SupportedTest' finished
```

TC8 - *TokenEndpoint.IsAsymmetricClientAuthenticationUsedTest*

This test determines whether the server supports asymmetric client authentication, such as mTLS or 'private_key_jwt'.

Requirement Level(s)

- SecBCP: **Should**

Test result

- Does the server support asymmetric client authentication: **NO**
- Test status: **FAILED**

Test log

```
Test `TokenEndpoint.IsAsymmetricClientAuthenticationUsedTest' started

  ✗  Test 'TokenEndpoint.IsAsymmetricClientAuthenticationUsedTest' was executed and failed.

Test `TokenEndpoint.IsAsymmetricClientAuthenticationUsedTest' finished
```