99_AllOauthDiagrams

All the figures/diagrams from various OAuth2 related specs and standrds.

Flows

The OAuth 2.0 and OIDC specifications (and related documents) contain various figures/diagrams.

This gist shows all of them together.

Image versions have been added for ASCII/text based version

draft-oauth-dpop.md[#](#)

```
# OAuth 2.0 Demonstration of Proof-of-Possession (DPoP) at the Application
Layer

```
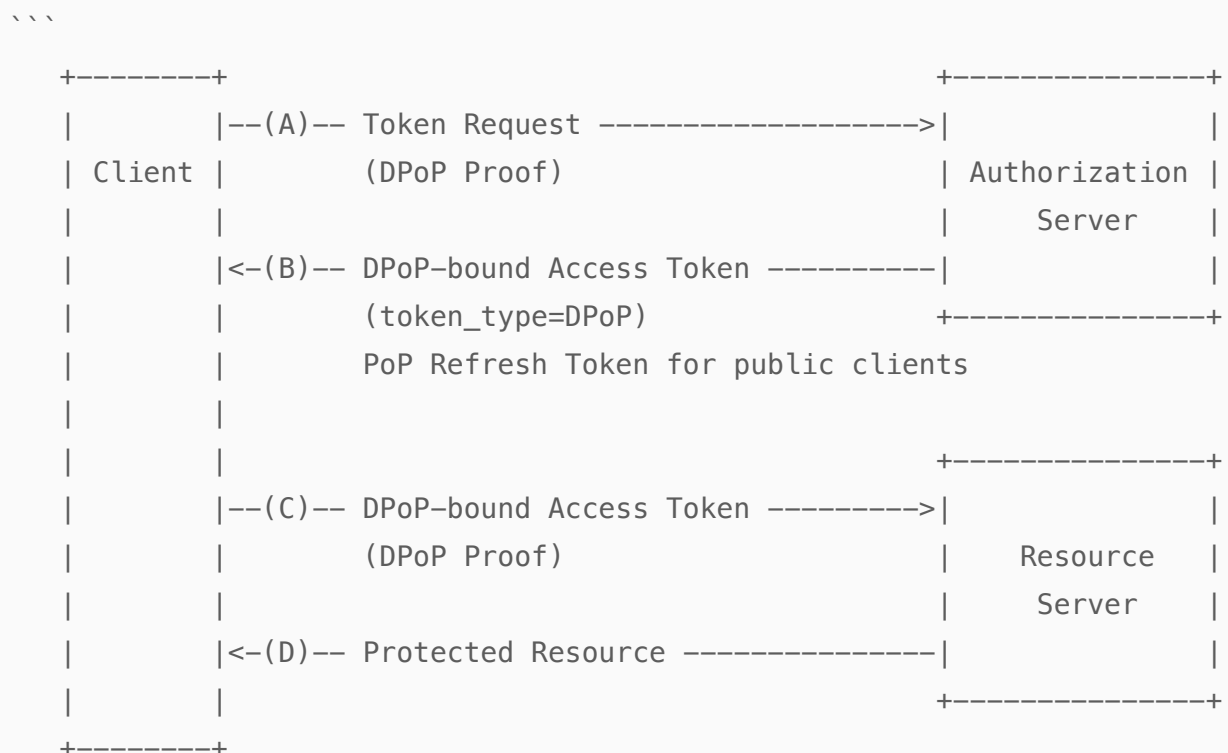
  +--------+                                          +--------------+
  |        |--(A)-- Token Request --------------------->|              |
  | Client |        (DPoP Proof)                        | Authorization |
  |        |                                            |    Server    |
  |        |<-(B)-- DPoP-bound Access Token ----------|              |
  |        |        (token_type=DPoP)                   +--------------+
  |        |        PoP Refresh Token for public clients
  |        |
  |        |                                            +--------------+
  |        |--(C)-- DPoP-bound Access Token ---------->|              |
  |        |        (DPoP Proof)                        |   Resource   |
  |        |                                            |    Server    |
  |        |<-(D)-- Protected Resource ---------------|              |
  |        |                                            +--------------+
  +--------+


                Figure 1: Basic DPoP Flow
```

```
![](https://www.plantuml.com/plantuml/png/jPDHQiCm44J_Uuhvj36wGHlY9WSmRl-
B8w-
9QV2cqghGeiCNfO85fmKLclTdh1tjpA2jby79ECimt05eJAP1AJgJQP9GH2OQKxMrCNZcLrhGqri
WBp3NRE9AE7uBxKupBQAArRxZ3frZdchyI4GRvCXk_XnavYKBwTyYzEWJkNTo0DP2zwPwJDRIGkR
0OHdHMalUPxFgxHTh6RKcQUv5Fixqa4JhluQDJ4gefycHF-PT9dOuXyDfjh2NGBrENY_qd-
tlYYBQ54HKsZw0dZm7PmcuPVlxPArpB6I5HhtKAAlsRn1serzRMiRBM_u2)

Source: [https://tools.ietf.org/html/draft-fett-oauth-dpop]
(https://tools.ietf.org/html/draft-fett-oauth-dpop)
```

OIDC-core.md#

```
# OpenID Connect Core

## Abstract Flow
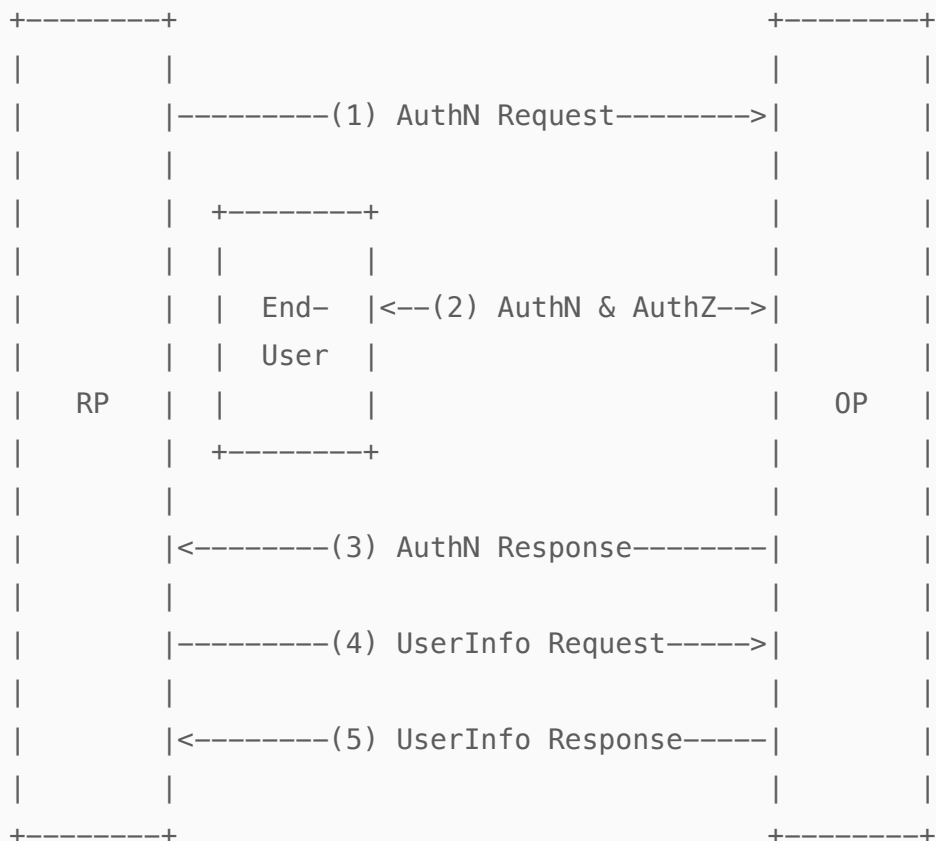
```
+--------+   +--------+
	---------(1) AuthN Request------->	
	+--------+	
		End- |<--(2) AuthN & AuthZ-->|
		User		
RP				OP
	+--------+	
	<--------(3) AuthN Response-------	
	---------(4) UserInfo Request---->	
	<--------(5) UserInfo Response----	
+--------+   +--------+
```
```

![]
(https://www.plantuml.com/plantuml/png/SoWkIImgISaiIKpaqjQ50cq5mW2XcAi69bP3X
3w4OYHzkZ2WOQYfu5XQak6d49HQM9fQN0AJi4Cefe9zoCudJH-2JR8-
rxmKNI331kXB8vWlrS1q52x_WL5eSMeHqVO51P3WJly0YiA5ydYmWSUxCIBUYmloyufJOJ88nLHD
PoQQu73rp4lBHqbgTZJodod2FbGlKcuVsVdM8JKl1Ppp0G00)

Source: [https://openid.net/specs/openid-connect-core-1_0.html]
(https://openid.net/specs/openid-connect-core-1_0.html)

OIDC-native-sso.md#

```
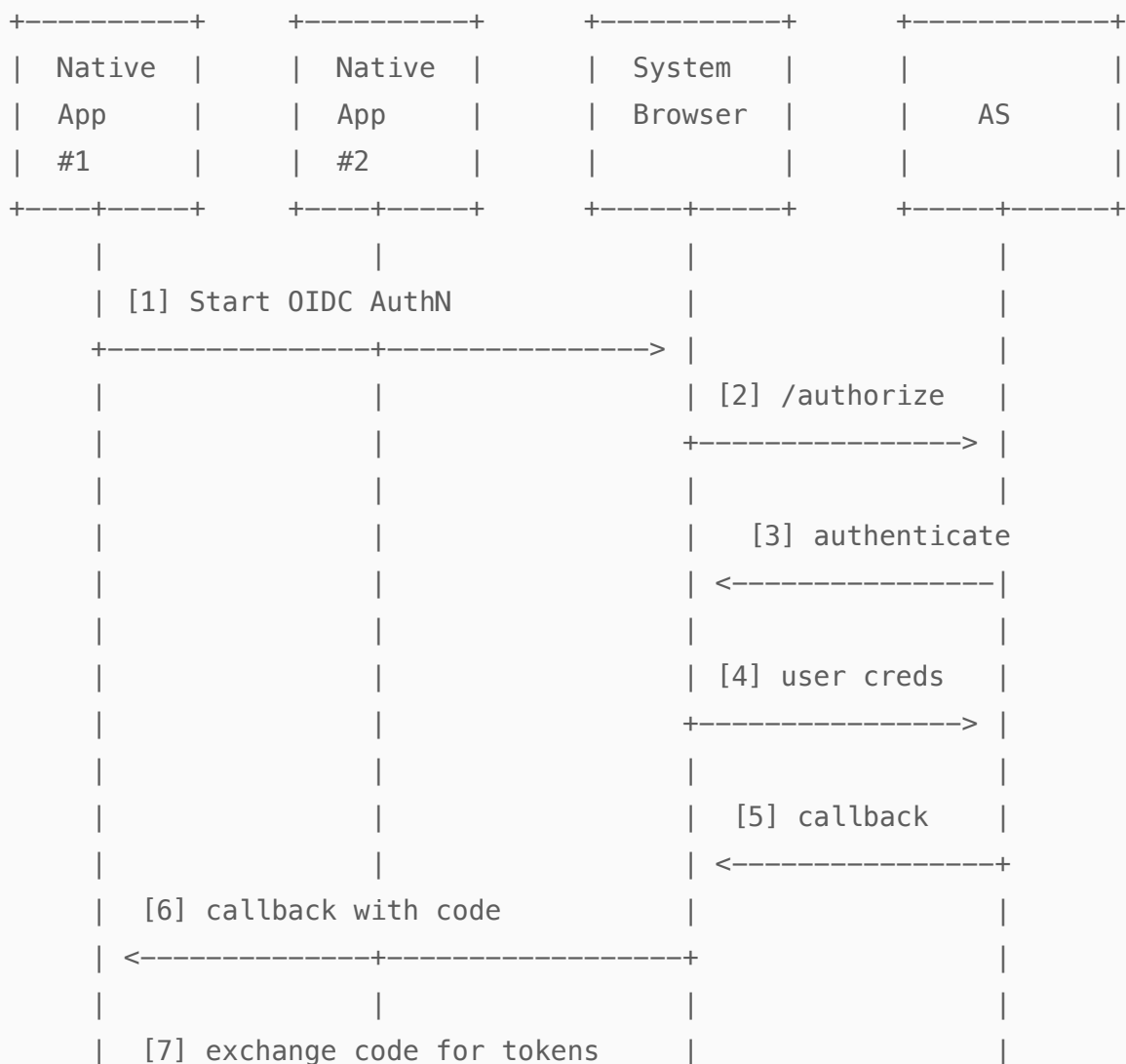# OpenID Connect Native SSO for Mobile Apps 1.0

## Abstract Flow

```

+----------+   +----------+   +-----------+   +------------+
Native		Native		System		
App		App		Browser		AS
#1		#2				
+----+-----+   +----+-----+   +-----+-----+   +-----+------+
     | | | |
     | [1] Start OIDC AuthN | |
     +-----------------+----------------> | |
     | | | [2] /authorize |
     | | +----------------> |
     | | | |
     | | | [3] authenticate
     | | | <----------------|
     | | | |
     | | | [4] user creds |
     | | +----------------> |
     | | | |
     | | | [5] callback |
     | | | <----------------+
     | [6] callback with code | |
     | <---------------+----------------+ |
     | | | |
     | [7] exchange code for tokens | |

```
          +---------------+----------------------------------> |
          |               |                      |             |
          |     [8] tokens (including device_secret)           |
          | <-------------+----------------+------------------+
          |               |                      |             |
          |               |                      |             |
          |               |                      |             |
          +               +                      +             +
```

![]
(https://www.plantuml.com/plantuml/png/rPLFImCn4CNl_HG3NfH5fFMF7egqwiLBFVGOW
iHaR4DhjYHfgz8FhzEoCfeWNTS_E9V0Rtbl7oyCwOMeV3GsAjKgzj-
c09e4S98YOgqLm415kq205T0aW8xXKuZu00onMP59VpPZNn90nuKlbm7zUvF-
a9dijBazWGu7_BVv99jE2ju91nNv154dYN4Uv56b5cq9GxeikBc-keJ-F8u7MwXP7ZO9EC-
gwoGN7Ga7wZLLwUqprbFduZHkhOPQ74gWwEYYrIfY7NNtO_PVJ2wE9Cnf1RH74_vLv-
9OWbRJwPtIapLgqZdRCN72V9SsZa6N1hTCtirl2KUf-
hjQ4wSIy56FbHlX9lHzwI6M4tIXyNxJ_EHzYpDPHTsrJa_dnheH65nOZRS1jSUuz-
NECwXvyhzL5vnbGHwrUkZC-hb-0G00)

Steps [1] - [8] are the standard OpenID Connect authorization_code flow with
the following extensions. In step 2, the device_sso scope is specified
signifying that the client is requesting a device_secret to be returned when
the code is exchanged for tokens.

```
+----------+     +----------+     +-----------+      +------------+
| Native   |     | Native   |     | System    |      |            |
| App      |     | App      |     | Browser   |      |     AS     |
| #1       |     | #2       |     |           |      |            |
+----+-----+     +----+-----+     +-----+-----+      +-----+------+
     |                |                 |                  |
     |                |                 |                  |
     |                | [9] token exchange                |
     |                +-----------------+----------------> |
     |                |                 |                  |
     |                |                 |                  |
     |                |     [10] refresh, access, [device_secret]
     |                | <---------------+------------------|
     |                |                 |                  |
```

```
     |              |                |                      |
     |              |                |                      |
     +              +                +                      +
```

![](https://www.plantuml.com/plantuml/png/jTJ1YeCm40RWUvvYO8zHMFUsi2pQ1-
Z5eqW9SLgbL2K9jWKVleo76fa62YN_PU2J-SbSpArJnZMTKqh8z1a950Q-
S28JCy1UkMv2W1ae36YKT-lm0ZwjcQca64Vl2mCQEpDSBPfjIL5w9L-
PNq_m0zkIDQzVibmdlNiPa8I9Xk353C8KQRlwhS4DP-
m1RxfL_GdVtvOf2wF_Q2__UBlAlcimU3HesmIKrcXj0bM3KwVnO54RT7Mmu8-
VpXB_zCZRqZSEGH8vzitoDta0)

Step [9] invokes the /token endpoint with the token exchange profile passing
the id_token obtained from the shared device storage, the client_id and the
device secret.

Step [10] returns the SSO generated refresh and access tokens for Native App
#2.

Source: [https://openid.net/specs/openid-connect-native-sso-1_0.html]
(https://openid.net/specs/openid-connect-native-sso-1_0.html)

RFC-6749.md[#](#)

```
# The OAuth 2.0 Authorization Framework


     +--------+                               +---------------+
     |        |--(A)- Authorization Request ->|   Resource    |
     |        |                               |     Owner     |
     |        |<-(B)-- Authorization Grant ---|               |
     |        |                               +---------------+
     |        |
     |        |                               +---------------+
     |        |--(C)-- Authorization Grant -->| Authorization |
     | Client |                               |     Server    |
     |        |<-(D)----- Access Token -------|               |
     |        |                               +---------------+
```

```
       |          |
       |          |                              +---------------+
       |          |--(E)----- Access Token ------>|    Resource   |
       |          |                              |     Server    |
       |          |<-(F)--- Protected Resource ---|               |
     +--------+                                   +---------------+
```

Figure 1: Abstract Protocol Flow

```
```

![](https://www.plantuml.com/plantuml/png/rPFVIiKm38VlVOfSReoyWOpD-
UTIcRv0wG8MfSKqKv0-l7GE2yN0WPsRyzsD9FoMZsQ8ObWM9yPSGQR3dGvqIcEX-
vrFi9CGcx5565Tv3Uo-ZRZWOQQFbQ80zhbnfXXMjhJrr_EWK-
gFNvuO_fs_nkQcnVe77jXu0KHCKD3p3-nVVv_1vwJlqwUgy9S_lJloSgBFP-
9FOitdROiP6Asb6E4bl947p5ocppjrd-opF51Iye_wlC_vyCH1o0ej9KxnUUm-1_BBTka_)

```
```

```
  +--------+                                        +---------------+
  |        |--(A)------- Authorization Grant --------->|               |
  |        |                                        |               |
  |        |<-(B)----------- Access Token -------------|               |
  |        |                & Refresh Token           |               |
  |        |                                        |               |
  |        |                        +----------+    |               |
  |        |--(C)---- Access Token ---->|          |    |               |
  |        |                        |          |    |    |               |
  |        |<-(D)- Protected Resource --| Resource |    | Authorization |
  | Client |                        |  Server  |    |     Server    |
  |        |--(E)---- Access Token ---->|          |    |               |
  |        |                        |          |    |    |               |
  |        |<-(F)- Invalid Token Error -|          |    |               |
  |        |                        +----------+    |               |
  |        |                                        |               |
  |        |--(G)----------- Refresh Token ----------->|               |
  |        |                                        |               |
  |        |<-(H)----------- Access Token -------------|               |
  +--------+             & Optional Refresh Token      +---------------+
```

Figure 2: Refreshing an Expired Access Token
```
```

![]
(https://www.plantuml.com/plantuml/png/pPJ1IiD048RlFiMSIi8oRo3IMclrfAWli2GZN
GoxCZljGVRXhJAK34GJATH-joJauz-
PsPbdyInj4Eyl01mg3gRZqEBseW9AGQmMjNw1nLOsYSE7bv0YhDb7WSD_LmKinOXWEh-
BBh6wraIQgcaePtX9RnG1-
_mfqGoUw9KfRzJKvqH7czWcDof2h9RrK75icyfHYQnel6itDS8Z9w56gDqNEwSjDmI8vV2W8ZDdA
bfsWQAC9dectX7t4kcRmHgjpgv6jpN2VTpvBhIQPyMS6D2AJZL7C9tHWLoRIsll6k9_h96x8zR8u
AgTmSFxryZwpfxlvrKxfzX-R-zF)

```
    +----------+
    | Resource |
    |   Owner  |
    |          |
    +----------+
         ^
         |
        (B)
    +----|-----+          Client Identifier      +---------------+
    |          -+-----(A)-- & Redirection URI ---->|               |
    |  User-   |                                  | Authorization |
    |  Agent   -+-----(B)-- User authenticates --->|    Server     |
    |          |                                  |               |
    |          -+-----(C)-- Authorization Code ---<|               |
    +-|----|---+                                  +---------------+
      |    |                                         ^        v
     (A)  (C)                                        |        |
      |    |                                         |        |
      ^    v                                         |        |
    +---------+                                      |        |
    |         |>---(D)-- Authorization Code ---------'        |
    | Client  |          & Redirection URI                    |
    |         |                                               |
    |         |<---(E)----- Access Token --------------------'
    +---------+          (w/ Optional Refresh Token)
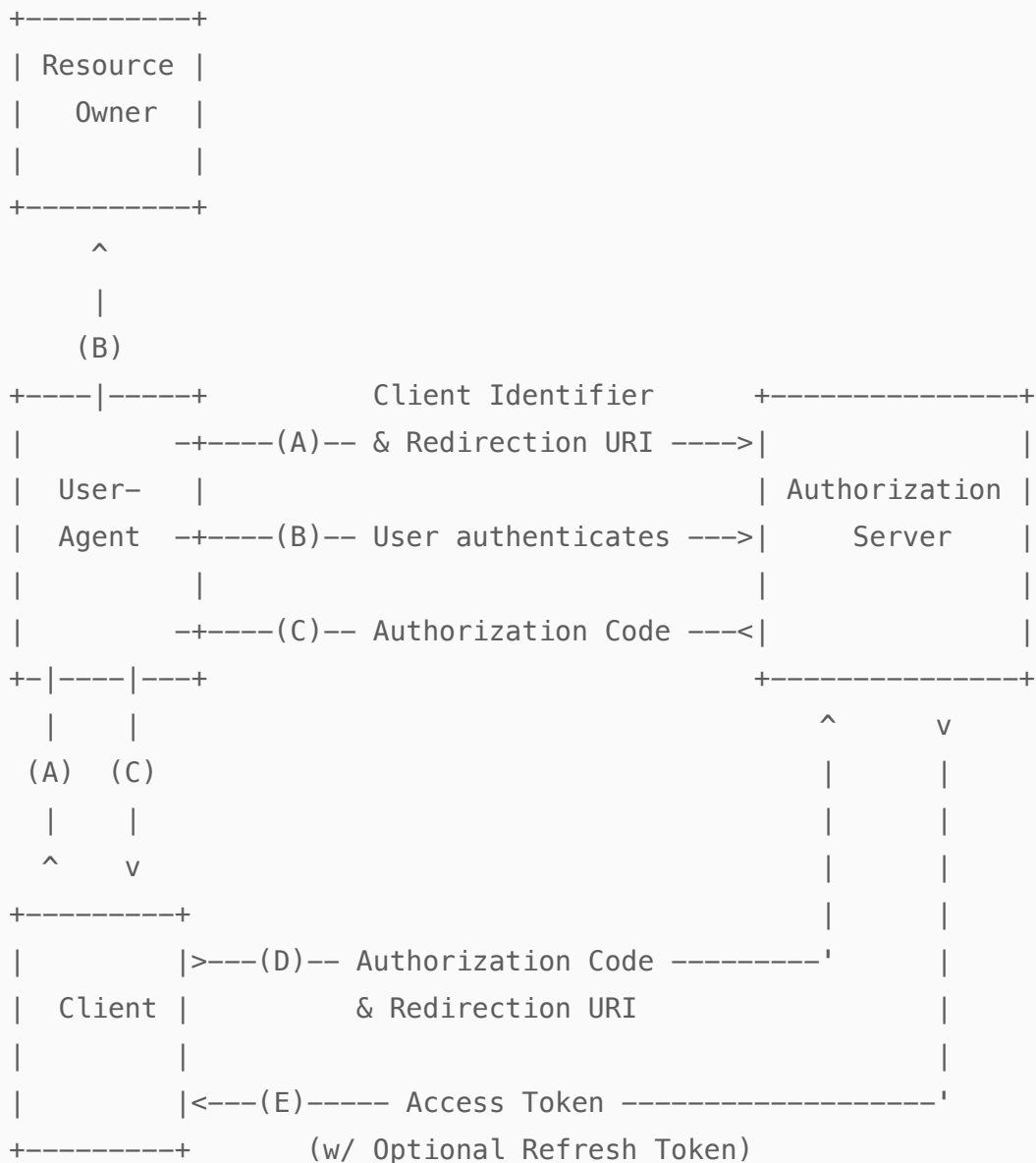
   Note: The lines illustrating steps (A), (B), and (C) are broken into
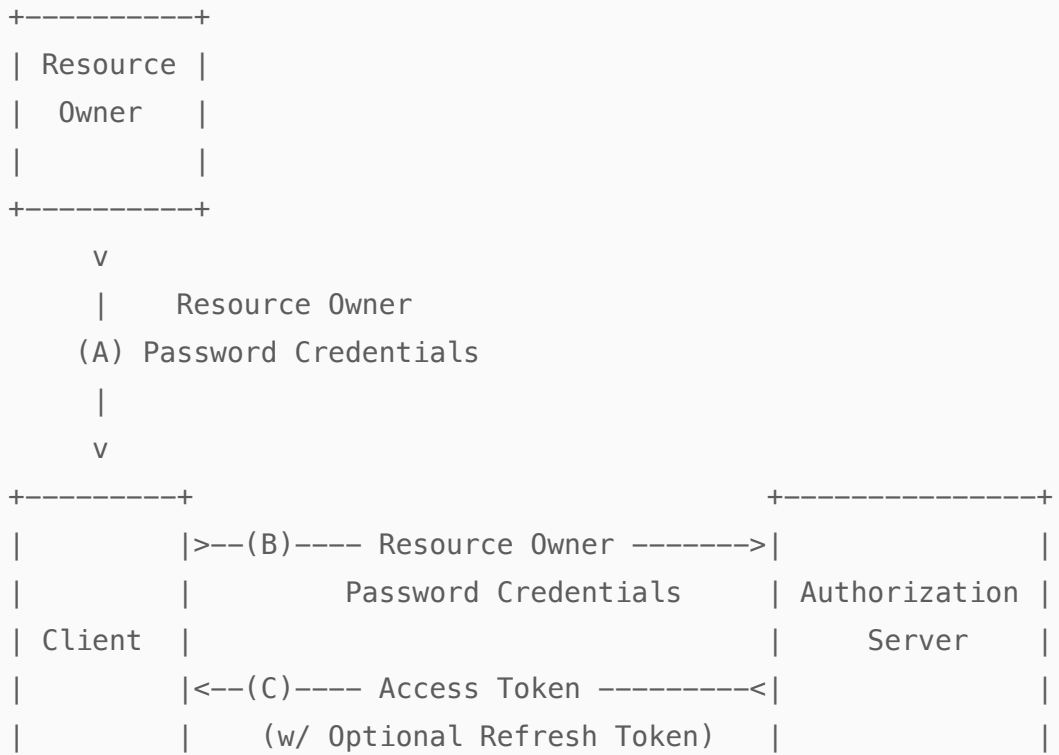   two parts as they pass through the user-agent.
```

Figure 3: Authorization Code Flow

```

![]
(https://www.plantuml.com/plantuml/png/dPJHQi8m58RlVOh_QbfAs0k8MDqkl1AwUIk4z
ZZ3f1r9L1Xv-
3MDDWiXKFfTL3ZaF_cIGrmhpQMkXUPy1alE1d9NCIX9jLTP4Sop0kpl3Kduoe19z74SPz5AosAJ_
0iP5yF0zYAeqTZLtLUS14a4UqJ2JrY_0b5aZE459TL2KgL5s-
1Gxi0wLWOX_a07HP85xL8O55TzRgNuvNrptwFuijvFZutri6t1k_NsB1NNfE0zFaZUI0OUZf4U8I
Pn7rlh4IflsvginpBH8tT3iPySQT9pyIO6OpcYv_Q8TtC4EdcCn3n-
ejqdnPtDRM8yzvSn9MvyVMKd-
9QUe6CUneSdP30GFuY8U7Ua6HDVMldtZ5bGL1KfXS_scngmc7dgwXRtL-
n_h3Q_eAIJ97LsRRBPcfgw_plx0m00)


```
     +----------+
     | Resource |
     | Owner |
     | |
     +----------+
         ^
         |
        (B)
     +----|-----+   Client Identifier   +---------------+
     | -+----(A)-- & Redirection URI --->| |
     | User- | | Authorization |
     | Agent -|----(B)-- User authenticates -->| Server |
     | | | |
     | |<---(C)--- Redirection URI ----<| |
     | | with Access Token   +---------------+
     | | in Fragment
     | | +---------------+
     | |----(D)--- Redirection URI ---->| Web-Hosted |
     | | without Fragment | Client |
     | | | Resource |
     | (F) |<---(E)------- Script ---------<| |
     | | +---------------+
     +-|--------+
       | |
      (A) (G) Access Token
```

```
     |     |
     ^     v
  +---------+
  |         |
  | Client  |
  |         |
  +---------+
```
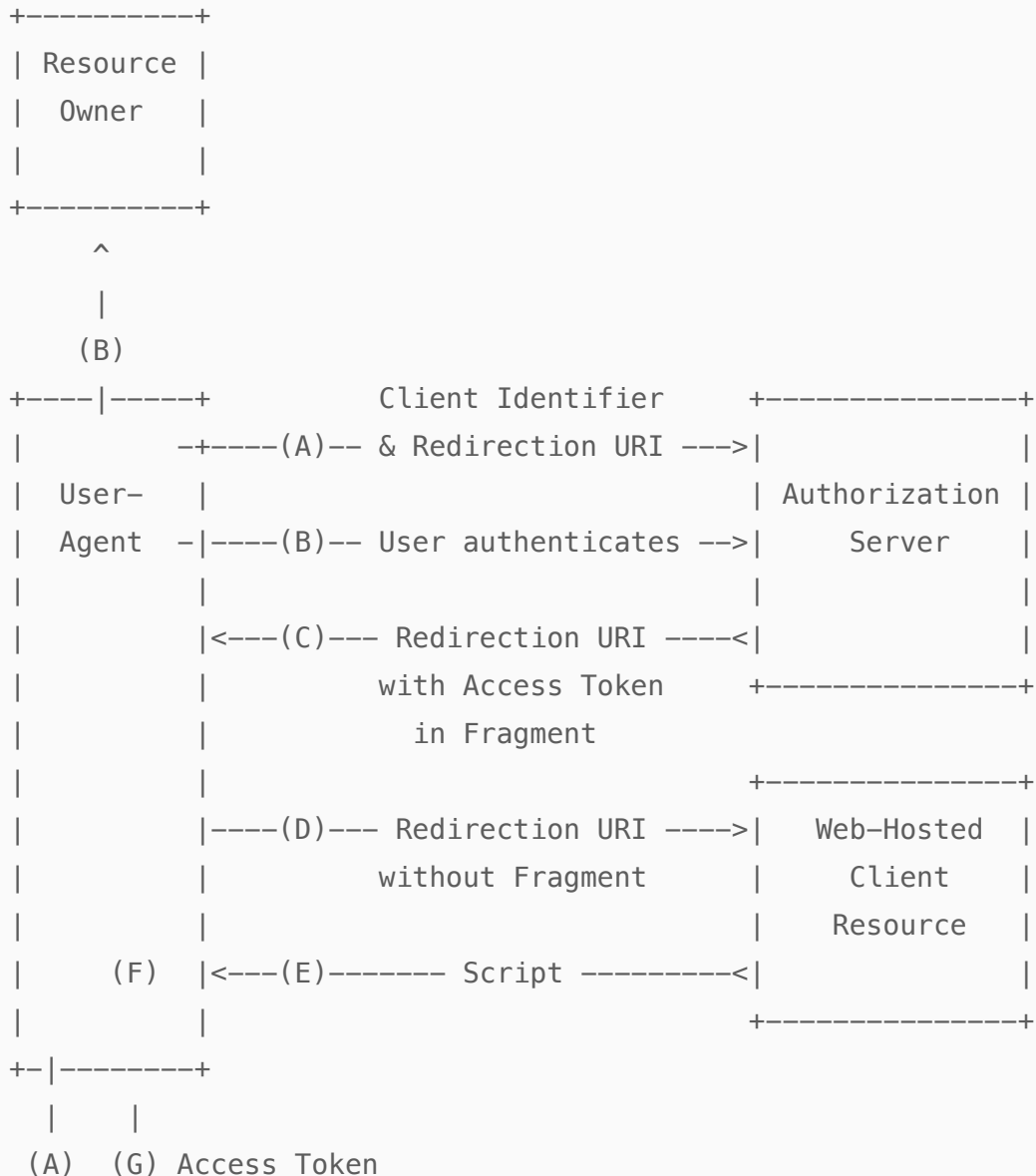
   Note: The lines illustrating steps (A) and (B) are broken into two
   parts as they pass through the user-agent.

                       Figure 4: Implicit Grant Flow
```

![](https://www.plantuml.com/plantuml/png/fLHDQm8n4BtxA-PKDiZ-0ockjhQU2bhfJKXtfnhQ9YKP5Kf-V3SHn_WHsE8xp64Stxpt9Zfq92qrYgJiGK2_PFJt7GypT6PZQmH_wC3BJgC5E7OOFiSJiUnTJ0OK8v5ypP-ivv9k6Nyfr0JJfgtgGw4zNtf14R5l5vKeIxY36JRAOatAQ5ZCfk7JUmyfKeCBXpPboy93jQ6riUfN1kg4ebgX9bOn2YeYgspdWv5Q4ZfW5NEqMxHm6NCt5KTaA0P1nLYqzLeKvQ031J1sYjPGrJKw1w_c4tN-8daZIiF4ojKtQlgNuwwxOkuFMSSnzpTyBv-D8smwE3OROiKymE_pXjFnZ-wSefY8m-aUHRa7p6khVWZOUlvq_hOuGzid7URY5L1KeYrFukGnN9s4PIZR0s_kRYoUO_MPYPHZYBg9_sj_)

```
    +----------+
    | Resource |
    |  Owner   |
    |          |
    +----------+
         v
         |    Resource Owner
        (A) Password Credentials
         |
         v
    +---------+                                +---------------+
    |         |>--(B)---- Resource Owner ------->|               |
    |         |          Password Credentials  | Authorization |
    | Client  |                                |    Server     |
    |         |<--(C)---- Access Token ---------<|               |
    |         |     (w/ Optional Refresh Token) |               |
```

```
      +---------+                                      +--------------+
```

                  Figure 5: Resource Owner Password Credentials Flow
```

![]
(https://www.plantuml.com/plantuml/png/fP9HQiCm38RVUmez9WIp2vJIB0Vew7O1asZKB
DX3SXiOESTEizFi9AkdkG8JoA3VaoFz-
QK_yPwZfJYuQEq64esvqKXbXYDoE5EFCESA72QF1A2L6_EYJ-
RxyqkVvBNiBfxQhTeQdYpp56Y0Zd107vqTULFE4Yxbt0RMK76PE3FlZAaUwzGhzWGZx4Iib5z4Ju
jf_YJjEPu2kGyRNV3gqOtkgakdLKJoZ7H1MjvZUytIIPQsxv4PNi8RUZ2PxV-
oLDC37DxJedQ48xuIyaciQXMN7dV-bptwuVUM_W00)

```
     +---------+                                      +--------------+
     |         |                                      |              |
     |         |>--(A)- Client Authentication --->| Authorization |
     | Client  |                                      |    Server    |
     |         |<--(B)---- Access Token ---------<|              |
     |         |                                      |              |
     +---------+                                      +--------------+
```
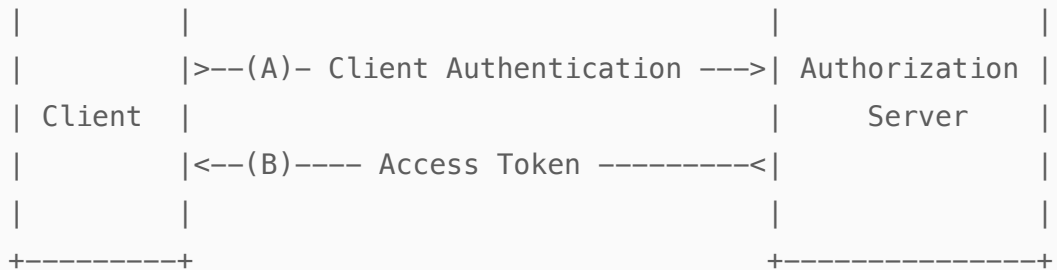
                       Figure 6: Client Credentials Flow
```

![]
(https://www.plantuml.com/plantuml/png/SoWkIImgISaiIKpaKW01RLqOq5R03n2A4LeWP
jI022YB8AX1vsEOOQUhg-
6egQlWd9EPcbUYu5XQaW6aCvCJIpBpynI0rjhLW0NpYpAhm69mCw1QI717S6fHMMeHTdVO0DtXf0
dofu9ZSd9gSR52I7vsAj05C623uHSgXGVbyUAGcfS2ZcK0)

Source: [RFC-6749](https://tools.ietf.org/html/rfc6749)

# RFC-6750.md[#](#)

```
OAuth 2.0 Bearer Token Usage

```

```
     +--------+   +--------------+
```

```
    |          |--(A)- Authorization Request ->|   Resource   |
    |          |                               |    Owner     |
    |          |<-(B)-- Authorization Grant ---|              |
    |          |                               +--------------+
    |          |
    |          |                               +--------------+
    |          |--(C)-- Authorization Grant -->| Authorization |
    | Client |                                 |    Server    |
    |          |<-(D)----- Access Token -------|              |
    |          |                               +--------------+
    |          |
    |          |                               +--------------+
    |          |--(E)----- Access Token ------>|   Resource   |
    |          |                               |    Server    |
    |          |<-(F)--- Protected Resource ---|              |
    +--------+                                 +--------------+


                  Figure 1: Abstract Protocol Flow
```

![](https://www.plantuml.com/plantuml/png/rPFVIiKm38VlVOfSReoyWOpD-
UTIcRv0wG8MfSKqKv0-l7GE2yN0WPsRyzsD9FoMZsQ8ObWM9yPSGQR3dGvqIcEX-
vrFi9CGcx5565Tv3Uo-ZRZWOQQFbQ80zhbnfXXMjhJrr_EWK-
gFNvuO_fs_nkQcnVe77jXu0KHCKD3p3-nVVv_1vwJlqwUgy9S_lJloSgBFP-
9FOitdROiP6Asb6E4bl947p5ocppjrd-opF51Iye_wlC_vyCH1o0ej9KxnUUm-1_BBTka_)

Source: https://tools.ietf.org/html/rfc6750

RFC-7521.md#

```
# OAuth 2.0 Client Authentication and Authorization Grants

```
    Relying
    Party                     Client                   Token Service
      |                          |                           |
      |                          | 1) Request Assertion      |
      |                          |-------------------------->|
      |                          |                           |
```

```
                         |   2) Assertion         |
                         |<-----------------------|
        3) Assertion     |                        |
|<-----------------------|                        |
|                        |                        |
        4) OK or Failure |                        |
|----------------------->|                        |
|                        |                        |
|                        |                        |
```
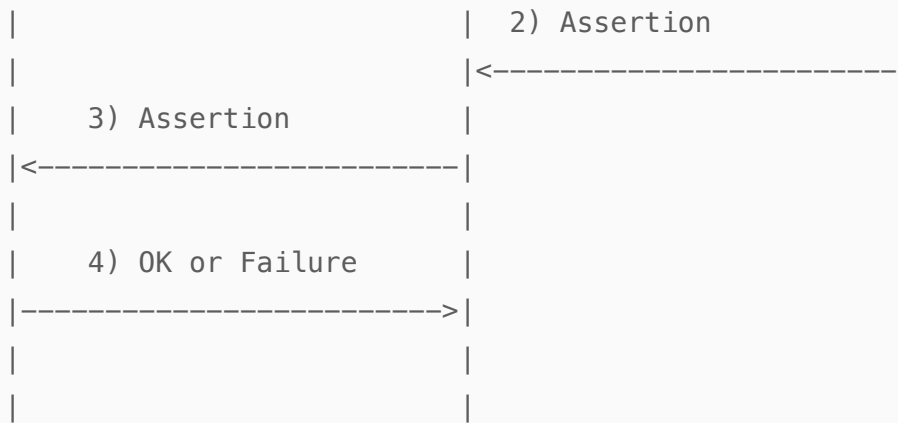
             Figure 1: Assertion Created by Third Party
```

![]
(https://www.plantuml.com/plantuml/png/SoWkIImgISaiIKpaKW21eDISoioyT0Wd02XNg
O0DEETafkQLO948oSzEpLC8JYqgoqnEvO8Arc1HI52gXZZTXff0DnUMfXQNA3WM5wSMbMJcvn6hM
nS7iAkXXykDD14k9bMt3Iwde-esHhE2iCi9Mg1BcR-
9rMsYgU3lhP1VfE2Mc9bJMfHAl6wS3hUZpEMqq-sGcfS2pe80)

```
    Relying
    Party                    Client
      |                        |
      |                        | 1) Create
      |                        |    Assertion
      |                        |-------------+
      |                        |             |
      |                        | 2) Assertion|
      |                        |<------------+
      |        3) Assertion     |
      |<-----------------------|
      |                        |
      |        4) OK or Failure |
      |----------------------->|
      |                        |
      |                        |
```

                  Figure 2: Self-Issued Assertion
```
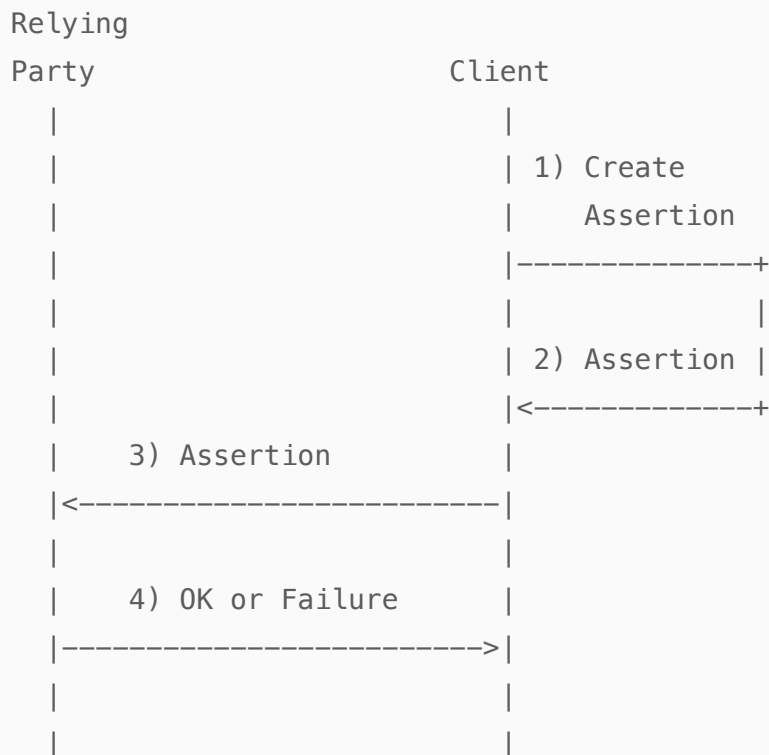
![]
(https://www.plantuml.com/plantuml/png/SoWkIImgISaiIKpaKW21eDISoioyT0Wd02XNg
O0DEETafkQLS45vDGeuGGqnQXGCDHMSYr8JIrA9KWq4ZiN5gKKbcVbvn6ZGHG7Qn6WXnnD6cWXd4
QV51e_3Z95CmtG9GYycg24vMamq5Voz5VAB5DmICtDAYrBHrU2qoevOkmYhSKZDIm6dGm00)

Source: [https://tools.ietf.org/html/rfc7521]
(https://tools.ietf.org/html/rfc7521)

RFC-7591.md[#](#)

```
# OAuth 2.0 Dynamic Client Registration Protocol

```
        +--------(A)- Initial Access Token (OPTIONAL)
        |
        |   +----(B)- Software Statement (OPTIONAL)
        |   |
        v   v
   +-----------+                                  +--------------+
   |           |--(C)- Client Registration Request -->|    Client      |
   | Client or |                                  | Registration  |
   | Developer |<-(D)- Client Information Response ---|   Endpoint    |
   |           |        or Client Error Response      +--------------+
   +-----------+
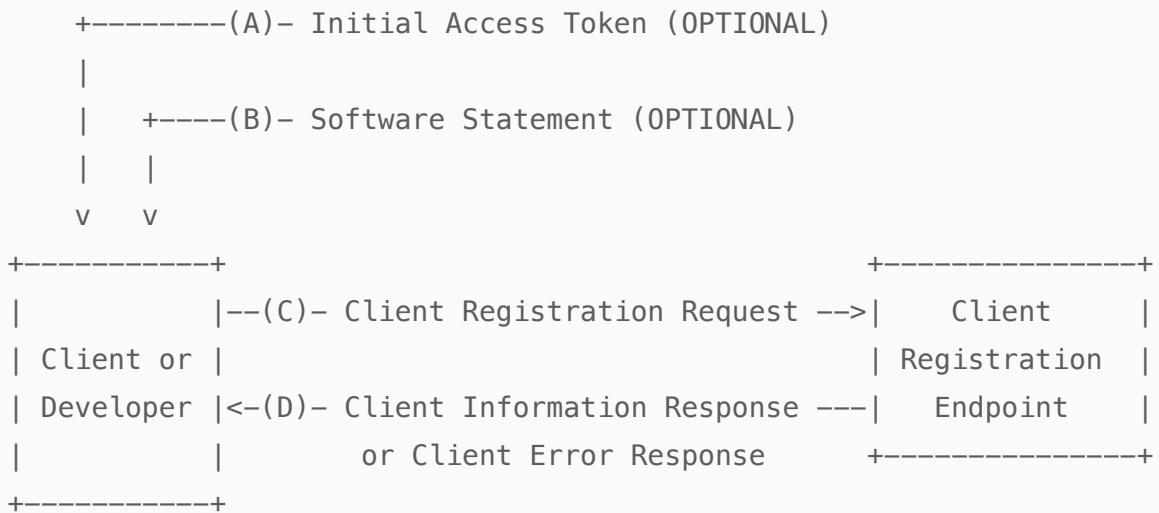
   Figure 1: Abstract Dynamic Client Registration Flow
```

![]
(https://www.plantuml.com/plantuml/png/XP9HQiCm38RVSmezfWJVO8ncRHy2OnrhBs0QT
PYbLYPhtKiEFtjK5O6H_M2GXVzFlutNIJnB7yJx2cvgt4rrktBGnI313z2UJfWI7Ea38zJxrsEtV
scVLtVNP9KowgViFz1PlZqZ7CGBNZ3Ad-
uPuLfMfLbK3VmlivYjqW6gAKVRv6YR8PGuR_WUah2NG35lFhym2JZtM2nwncuuQOlOeCkQPYCCjC
Kh3ZHY1ZsuUck9kdWclcYWD59C2CwvCcyN-v52YMIWkwmcLjYEcTWm2s_Kp3fhZFtln_W1)

Source: [https://tools.ietf.org/html/rfc7591]
(https://tools.ietf.org/html/rfc7591)
```

RFC-7592.md[#](#)

```
# OAuth 2.0 Dynamic Client Registration Management Protocol

```

        +---------(A)- Initial Access Token (OPTIONAL)
        |
        | +----(B)- Software Statement (OPTIONAL)
        | |
        v   v
    +----------+   +--------------+
    | |--(C)- Client Registration Request -->| Client |
    | | | Registration |
    | |<-(D)- Client Information Response ---| Endpoint |
    | | +--------------+
    | |
    | | +--------------+
    | Client or|--(E)- Read or Update Request ------->| |
    | Developer| | |
    | |<-(F)- Client Information Response ---| Client |
    | | | Configuration|
    | | | Endpoint |
    | | | |
    | |--(G)- Delete Request --------------->| |
    | | | |
    | |<-(H)- Delete Confirmation -----------| |
    +----------+   +--------------+
```

![[](https://www.plantuml.com/plantuml/png/hPJXQi8m58N_-
nJvMP6ymH2xrcs5COUw1mZsLi9gqYLNzwSFlwJqBXGx22CV20PwJaxE3TbO50PhYK8isCYAZsJva
hDAIPIYPVdf1DQoe_u4nRBT-
x7QlUMlorzL7_wHH_Rez0VTuBSmm0ue42wWS5OzSRZvtuAo42iM0qc2R44R4BsBLhXeHIjzd3sSf
KKZK6hb5bzNiCWuNti9VUFfxurO5FraYrcZ1vwL8L6b6cqk5CXsMbbmYRYNR5NTQQdmZqHfEaflJ
KVJPgX_wmwx1r7xzKTN2uJGl8VgdqbKmWrQtO69ht_AVFrF4VMdkn25LeqyNySRyM-
ZY0kHh2CtjMVNKGajt4-BM4SOfPpQIqWqL4fZuu4PerGFomPKFRoTFm00)

Source: [https://tools.ietf.org/html/rfc7592]
(https://tools.ietf.org/html/rfc7592)

# RFC-7636.md[#](#)

```
Proof Key for Code Exchange by OAuth Public Clients
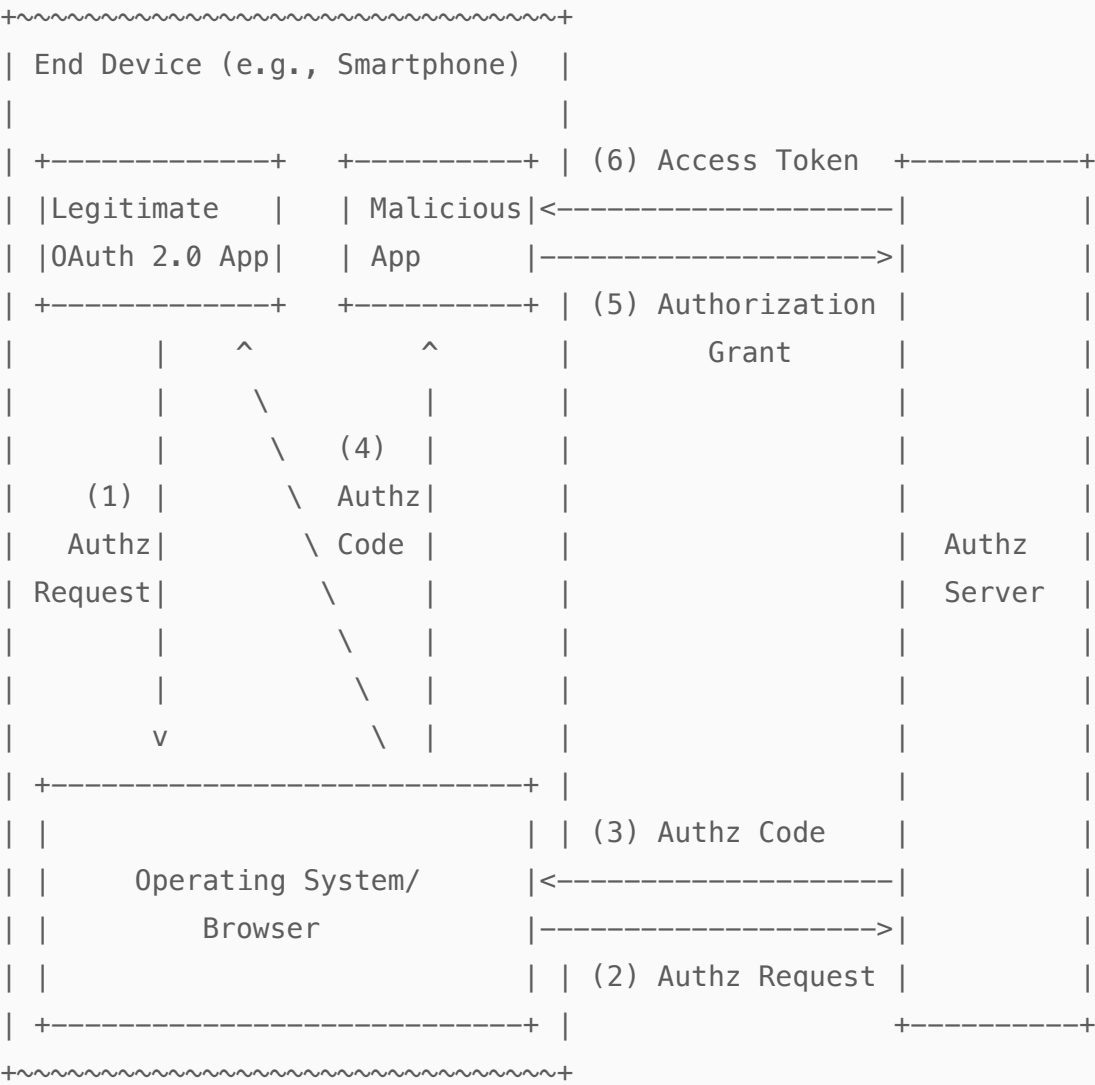
```

    +~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~+
    | End Device (e.g., Smartphone)     |
    |                                   |
    | +-------------+   +----------+ | (6) Access Token  +----------+
    | |Legitimate   |   | Malicious|<--------------------|          |
    | |OAuth 2.0 App|   | App      |-------------------->|          |
    | +-------------+   +----------+ | (5) Authorization |          |
    |        |      ^        ^      |       Grant        |          |
    |        |       \       |      |                    |          |
    |        |        \  (4) |      |                    |          |
    |    (1) |         \ Authz|      |                    |          |
    |   Authz|          \ Code|      |                    | Authz    |
    | Request|           \    |      |                    | Server   |
    |        |            \   |      |                    |          |
    |        |             \  |      |                    |          |
    |        v              \ |      |                    |          |
    | +---------------------------+ |                    |          |
    | |                           | | (3) Authz Code    |          |
    | |    Operating System/      |<--------------------|          |
    | |        Browser            |-------------------->|          |
    | |                           | | (2) Authz Request |          |
    | +---------------------------+ |                    +----------+
    +~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~+


           Figure 1: Authorization Code Interception Attack
```

![]
(https://www.plantuml.com/plantuml/png/hPHDJuGm48Rl_eevGb3KzUDapE97l6Ws4O-
RJHgOi8tIObimRlZn5hRima80nJaGwBnzsfbXPYuL4IgaYf0ZqEQS39XJod9uP24yO4O310lTo3q
6FzQaPCqPsbfWP0DMoPh7EisBE5fWNTlW1G5A2M_y7LbJO2ZvCqPKqPWeD8Vdy48-
Q41vAlERhd3ozbtoXPUgDSpSC_2IP4lHBqRK1Rdje0n7TAKZqWTnGJT4KSwWWr9z5e_LthsghnVs
90XJ1slTbBhxa09jNo_5khJ_Gh7ExJgbICBcrvJzhgtxdeSuT9ToJutoYfyfIbMgbwOqoy68V1GP
Ykwyr3ucP7So9Pj6wHq2pbXAR_CNRkl2DYKfYzT7MIGeT9Em2FnlgJ0-
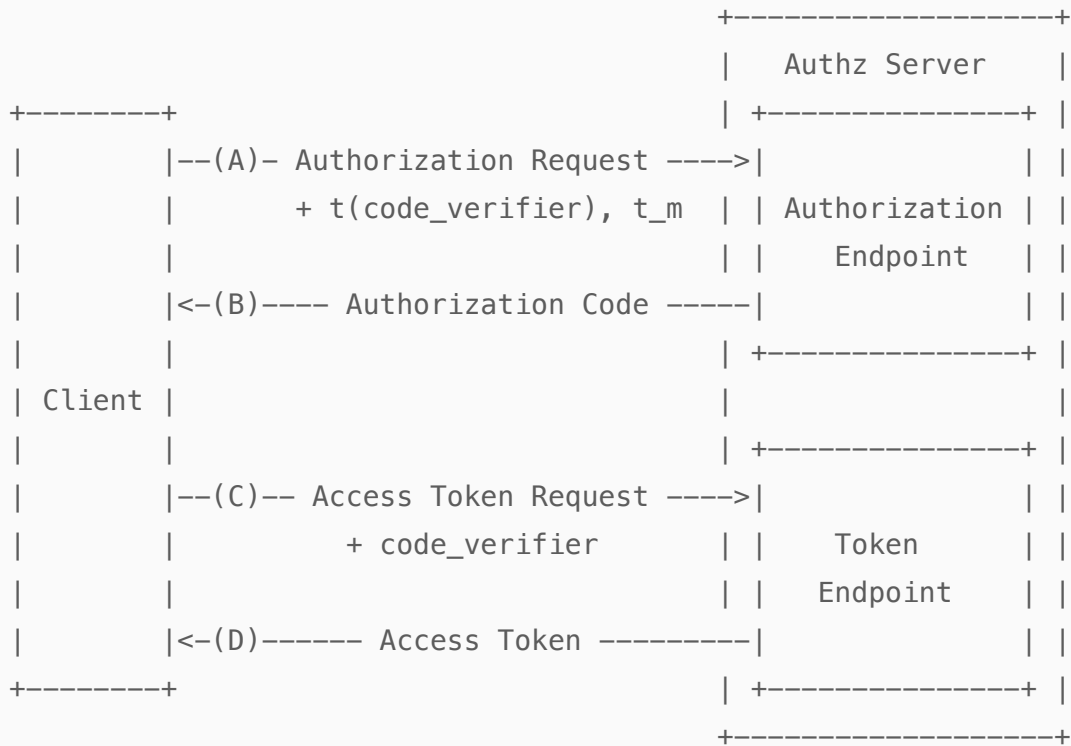DQBHFRrRkHFyInRbgud6zlHmHBCg8lDh_LDsMxDkn9YU8mlBkVu3)

```

                                                   +-------------------+
                                                   |   Authz Server    |
            +--------+                             | +---------------+ |
            |        |--(A)- Authorization Request ---->|               | |
            |        |       + t(code_verifier), t_m  | | Authorization | |
            |        |                             | |    Endpoint   | |
            |        |<-(B)---- Authorization Code -----|               | |
            |        |                             | +---------------+ |
            | Client |                             |                   |
            |        |                             | +---------------+ |
            |        |--(C)-- Access Token Request ---->|               | |
            |        |           + code_verifier   | |     Token     | |
            |        |                             | |    Endpoint   | |
            |        |<-(D)------ Access Token ---------|               | |
            +--------+                             | +---------------+ |
                                                   +-------------------+


                     Figure 2: Abstract Protocol Flow
```

![]
(https://www.plantuml.com/plantuml/png/hPH1Je0m44NtdA9BcjeR60EY5r3tfA5ZRDHMs
y45wU6jawYX24BA96oQykV_UUaq0PL7RL2fYXqj8PSbZil4zBKZFati7lm7U3ghyXxYVncHU_cLY
J-tfAnRBgcXysPIQ9nbT_0-Ga0cKrt5NFWlcMzx3El1QUYJR_DemFCBXlqh_PJrs9BP24LNRgr-
SyRYcfjBML_pv3tFrILh54hk3bKmukx5WCKzCeiwsKq6lEDVana6284zk6Se04xCPyJdf4Y-
QCHnndiT-0q1puFHqGRm4zzKwQAe6h2QLiyd)

Source: [https://tools.ietf.org/html/rfc7636]
(https://tools.ietf.org/html/rfc7636)

RFC-8252.md#

```
# OAuth 2.0 Device Authorization Grant

```

    +~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~+
    | User Device |
```

```
    |                    |
    | +-----------------------+ | (5) Authorization  +--------------+
    | |                       | |     Code           |              |
    | |      Client App       |-------------------->|   Token      |
    | |                       |<--------------------|   Endpoint   |
    | +-----------------------+ | (6) Access Token,  |              |
    |   |          ^           |     Refresh Token  +--------------+
    |   |          |           |
    |   |          |           |
    |   | (1)      | (4)       |
    |   | Authorizat-| Authoriza- |
    |   | ion Request| tion Code  |
    |   |          |           |
    |   |          |           |
    |   v          |           |
    | +-----------------------+ | (2) Authorization  +--------------+
    | |                       | |     Request        |              |
    | |      Browser          |-------------------->| Authorization |
    | |                       |<--------------------|   Endpoint   |
    | +-----------------------+ | (3) Authorization  |              |
    |                           |     Code           +--------------+
   +~~~~~~~~~~~~~~~~~~~~~~~~~~~~~+
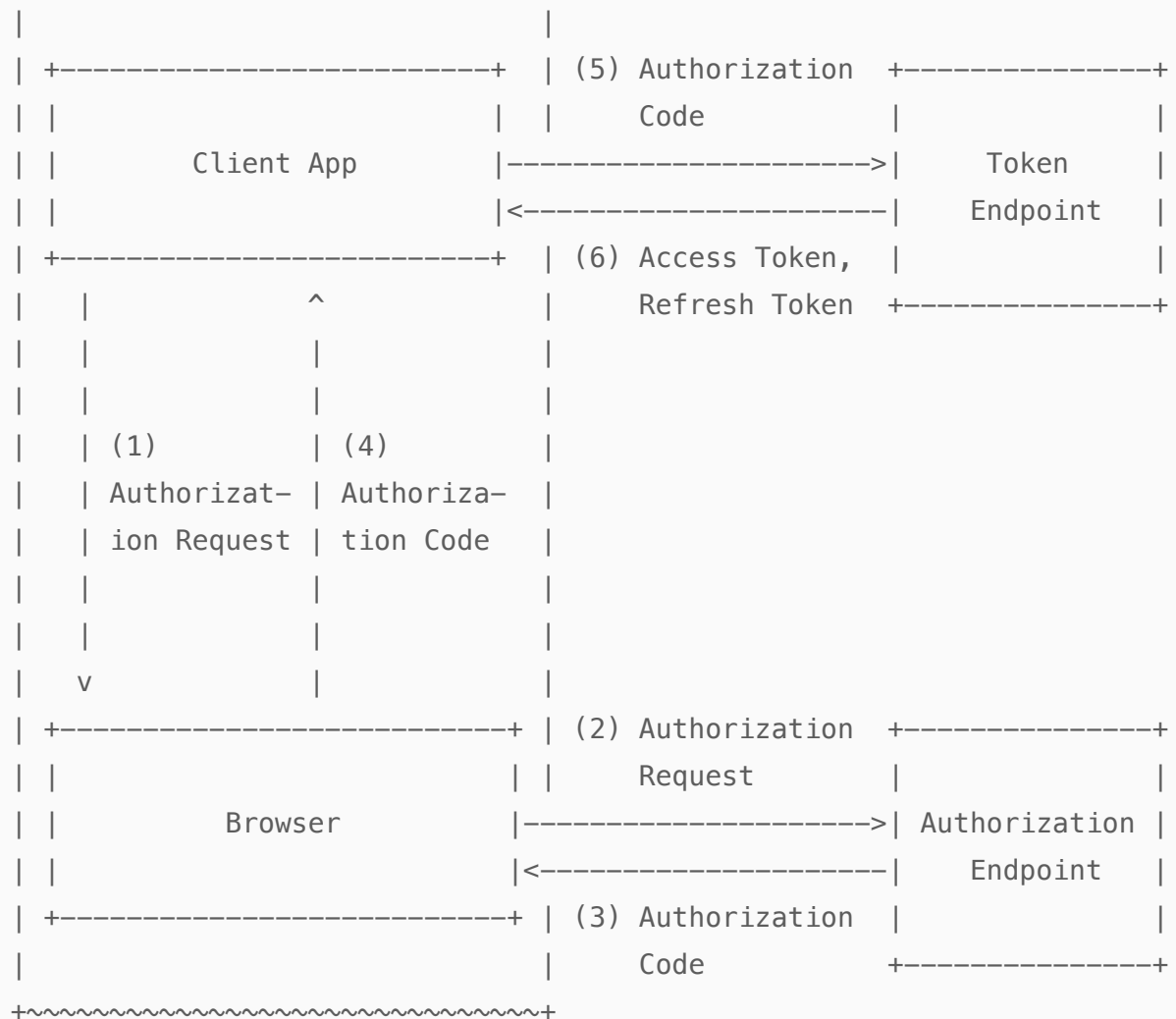

       Figure 1: Native App Authorization via an External User-Agent
```

![]
(https://www.plantuml.com/plantuml/png/hLJBJiCm4Bpp5Juc2ZxmW5E5MWe_KC4LAKeMr
GBPmTuM2VdZIMfriQoD3Q9pM-
_4dfsClNJOMkmLjksP48tCenavNX2U7LZn07lLWI1uul0WJkwqPkfNDxLOxN1hhFfgKHcT22H1cU
FyKSpQz12liufeTVskGADO3GCH98kxyCcJUGCTU4L52ydYyCcZxWUZDFxUezlHewu3vuA6yxdHql
KNGQ3U1bujk6tOYJERsIYj_iIfBkg8KrtN3ESd0JAkPCoPih61Znqu72iSo-
F_zYVMl2znidUecQQy_7UggKj35r9DkBVcqu6D63EfJYJwigB52L9D7bqb7isDbWDxytcpo-
_U4dH_U2M_0G00)

Source: [RFC-8252](https://tools.ietf.org/html/rfc8252)

RFC-8628.md[#](#)

OAuth 2.0 Device Authorization Grant

```
      +----------+                                +---------------+
      |          |>---(A)-- Client Identifier --->|               |
      |          |                                |               |
      |          |<---(B)-- Device Code,      ---<|               |
      |          |              User Code,        |               |
      |  Device  |         & Verification URI     |               |
      |  Client  |                                |               |
      |          |    [polling]                   |               |
      |          |>---(E)-- Device Code      --->|               |
      |          |            & Client Identifier |               |
      |          |                                | Authorization |
      |          |<---(F)-- Access Token     ---<|    Server     |
      +----------+   (& Optional Refresh Token)   |               |
           v                                      |               |
           :                                      |               |
        (C) User Code & Verification URI          |               |
           :                                      |               |
           v                                      |               |
      +----------+                                |               |
      | End User |                                |               |
      |    at    |<---(D)-- End user reviews  --->|               |
      |  Browser |          authorization request |               |
      +----------+                                +---------------+
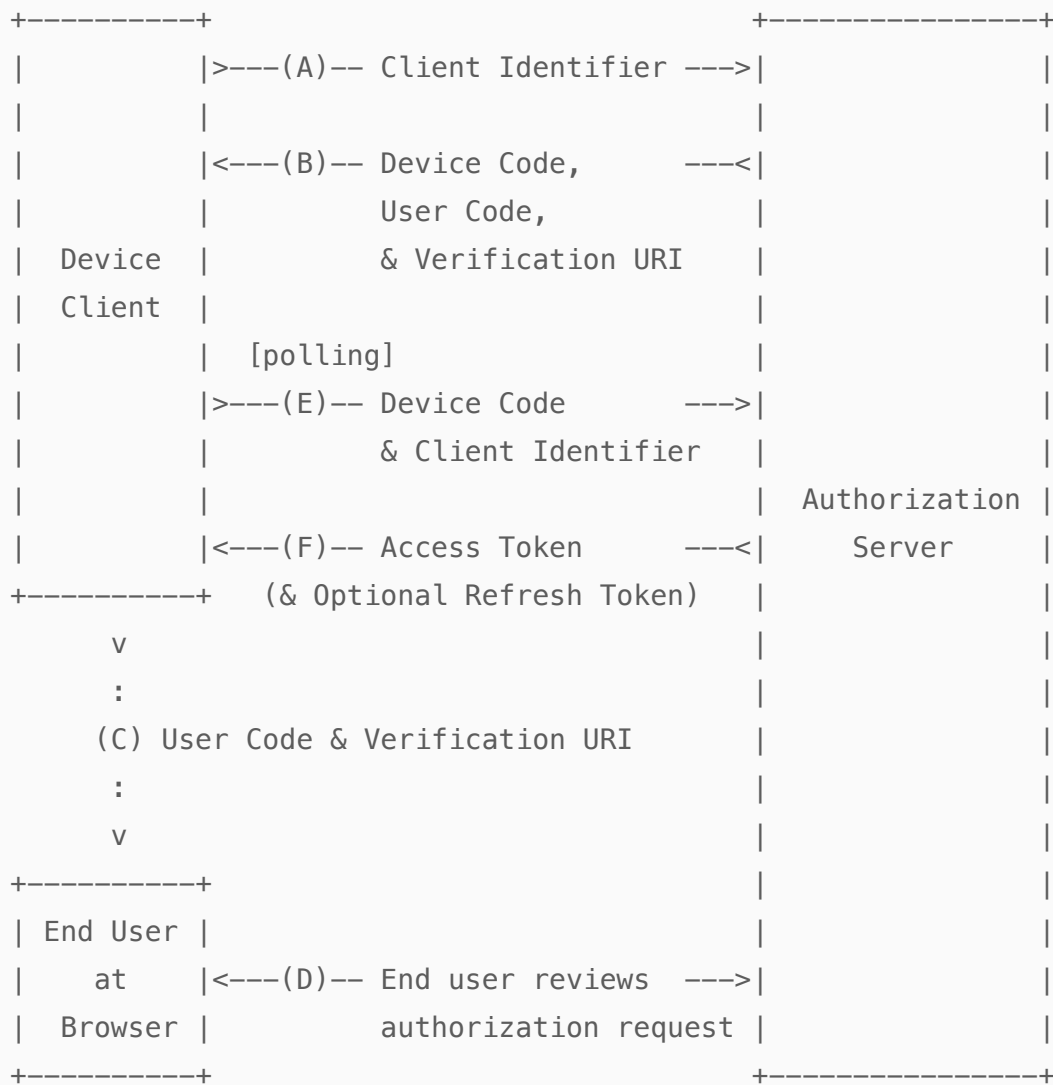
                    Figure 1: Device Authorization Flow
```

![]
(https://www.plantuml.com/plantuml/png/hLNBJiCm4Bpp5NkA4eNy0AggfccHUa8gb0lYO
2LRQX7PPUsa4ih74zUe3ojWIZs77BBHU7PsDfuepKXNN3Ds0tkasG4fU91c3j9laWuEwCRz-
pXFiWoAcgFGiAZw9rzp9EXBumuST0CauC6VI4P6oTGecM7BIuH2LdXhYtrfTA6IbK8wfV0hiSUUV
HF1Cr9lHiaqbm9MouMFnBeOoXE0bwsiQoxUNYybSKOyTuorjV-
CE1f82a2edEIDtaZYdzRm7tDoRzh9onALWYVvZiBDoIDIYtIgnDsTE8A7hJc5rR34DQ7QMAhajtO
iMl33It8NW2GkacFIX-
CQNabmJzpfNB4xSr5PGwvSGAQFOPkPi1dYnX0JjXntohyxKv8xHmaxIpVXHuDA3oW9yxUVeAZsby
SN)

```
            +-------------------------------------------------+
            |                                                 |
            |   Using a browser on another device, visit:     |
            |   https://example.com/device                    |
            |                                                 |
            |   And enter the code:                           |
            |   WDJB-MJHT                                      |
            |                                                 |
            +-------------------------------------------------+


                  Figure 2: Example User Instruction
```

![]
(https://www.plantuml.com/plantuml/png/fTAn2i8m4CRnlK_nxRLsxrJ5GGfkYlFP72PWB
oKvgaCVNj15HIWX__r7FiYrKIceSKfKuAEoIglyqZFIcd_rAJgvWd09_Xuvm0j8l5eEC3ovdbUON
7JQ_DLMTOnDNVE3Xl76wzuFzPijlvsxV2C6BCe1QXczDzmawFEksrQ7Rd_4SldBi_wxQ5dCwt2U)

```
            +----------------------------------------------------+
            |                                                    |
            |   Scan the QR code or, using    +------------+  |
            |   a browser on another device,  |[_]..  . [_]|  |
            |   visit:                        | .  ..   . .|  |
            |   https://example.com/device    | . .  . ....|  |
            |                                 |.   . . .   |  |
            |   And enter the code:           |[_]. ... .  |  |
            |   WDJB-MJHT                     +------------+  |
            |                                                    |
            +----------------------------------------------------+


      Figure 3: Example User Instruction with QR Code Representation
                 of the Complete Verification URI
```

![](https://www.plantuml.com/plantuml/png/fP8_IyOm4CPtFyMpz-
rrxrJ5GGeE_W474Od9OGCsASbP7VBXjH6aQgIKzvSbou_dxk6wA2g8iQBK2LPKzLwg7tx2Nj9l_q
Oh1naOLzVGtZ1yEE0rMlVyTyAgu2iy1VyMES0xAETbu033izLy093k7n-
80CBd9nNysKOhBVuZOP49085A_Y0onRPf-

```
5sDqmkJzcFp5V_jKvQ9Ylu6AKVd1vJyKsV0JZWi9UO6ryla_NCugEpVdVTdzML_SOiIs_tl91rzV
nqxao_v0m00)

Source: [https://tools.ietf.org/html/rfc8628]
(https://tools.ietf.org/html/rfc8628)
```

RFC-8705.md[#](#)

```
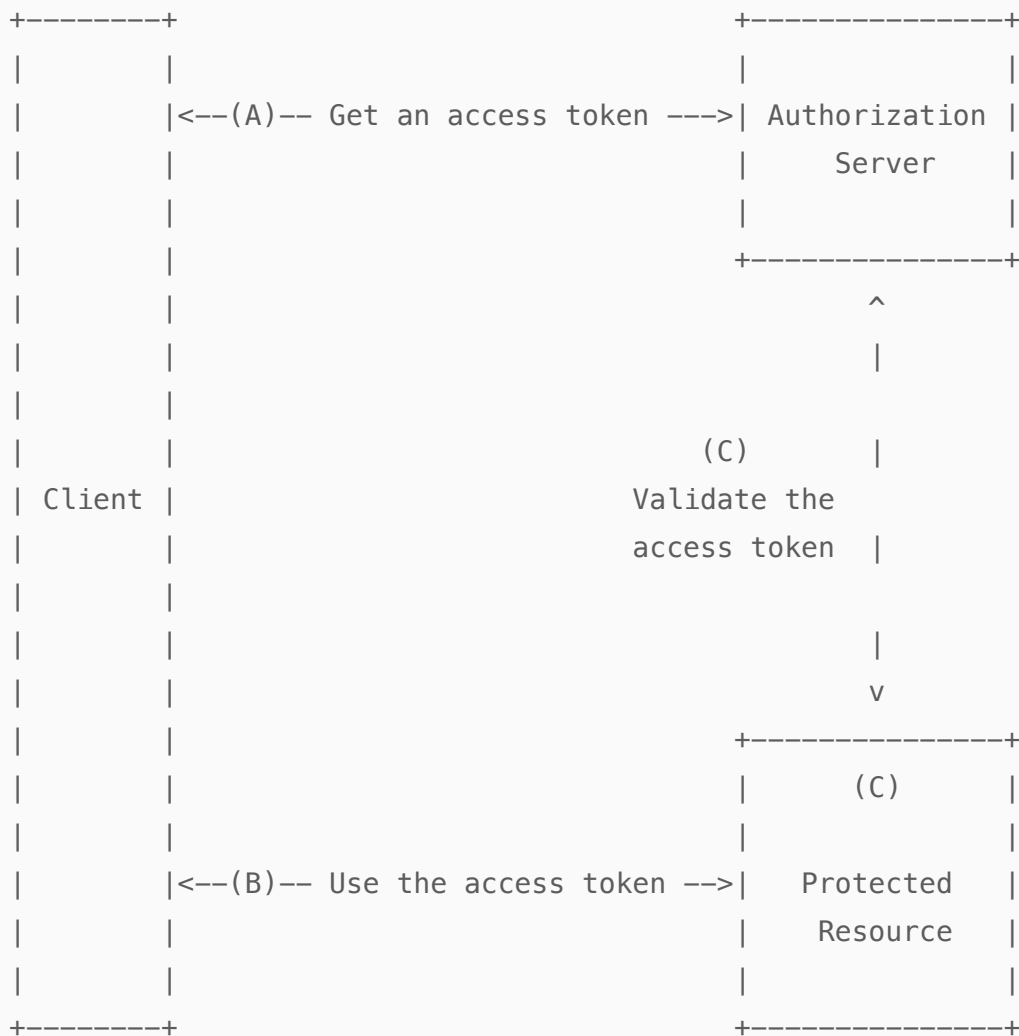#      OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound
Access Tokens

```
```
    +--------+                                      +--------------+
    |        |                                      |              |
    |        |<--(A)-- Get an access token --->| Authorization |
    |        |                                      |    Server    |
    |        |                                      |              |
    |        |                                      +--------------+
    |        |                                             ^
    |        |                                             |
    |        |                                             |
    |        |                                    (C)      |
    | Client |                                 Validate the
    |        |                                 access token  |
    |        |                                             |
    |        |                                             |
    |        |                                             v
    |        |                                      +--------------+
    |        |                                      |    (C)       |
    |        |                                      |              |
    |        |<--(B)-- Use the access token -->|   Protected  |
    |        |                                      |   Resource   |
    |        |                                      |              |
    +--------+                                      +--------------+


              Figure 1: Abstract OAuth 2.0 Protocol Flow
```
```
![](https://www.plantuml.com/plantuml/png/nLH1IyOm3Br_loB7ZT5_86Dp1w-
```

Yw548RM35heKstK7wutLgGNfms4rzjzAyv2Nfwn0OFSV5N9Hcn0jiwCGdEjX33iteFZAaV9zW3wa
ybnckX6Z6LWYu8GQqW59I2C3kcIoybUmJZ95dv_KBidOMKgM6U_8h-QpXv2x-
O98PJzNChBgsYsPgI-PaD5d-blc8HYja0fxf1mM_leFZqW6ECzT_M7eg9fz-
nu3Ncm4VmlkEIWVsM-YjTqoIITLhkAFWefTqKXV7lxA1h8gBUGK0)

Source: https://tools.ietf.org/html/rfc8705

W3C-IndieAuth.md[#](#)

```
# IndieAuth

![Authentication using the Authorization Code Flow]
(https://www.w3.org/TR/indieauth/authentication-flow-diagram.svg)

![Access token using the Authorization Code Flow]
(https://www.w3.org/TR/indieauth/authentication-flow-diagram.svg)

Source: [https://www.w3.org/TR/indieauth/](https://www.w3.org/TR/indieauth/)
```