4.2.1. [illegible](4.2.1. Authorization Request)

4.2.1. [illegible]

[illegible]
[illegible]B"application/x-www-form-urlencoded"[illegible]URI[illegible]URI[illegible]

- response_type
  [illegible]"token"[illegible]
- client_id
  [illegible]
  2.2
- redirect_uri
  [illegible]
  3.1.2
- scope
  [illegible]
  3.3
- state
  [illegible]
  10.12

[illegible]HTTP[illegible]URI[illegible]URI[illegible]

[illegible]TLS[illegible]HTTP[illegible]

```
GET /authorize?response_type=token&client_id=s6BhdRkqt3&state=xyz&redirect_uri=https%3A%2F%2Fclient
Host: server.example.com
```

[illegible]3.1.2[illegible]URI[illegible]URI[illegible]

[illegible]HTTP[illegible]URI[illegible]URI[illegible]

4.2.1. Authorization Request

The client constructs the request URI by adding the following   parameters to the query component of the authorization endpoint URI   using the "application/x-www-form-urlencoded" format, per Appendix B:

response_type

REQUIRED. Value MUST be set to "token".

client_id

REQUIRED. The client identifier as described in Section 2.2.

redirect_uri

OPTIONAL. As described in Section 3.1.2.

scope

OPTIONAL. The scope of the access request as described by Section 3.3.

state

RECOMMENDED. An opaque value used by the client to maintain   state between the request and callback. The authorization   server includes this value when redirecting the user-agent back

to the client. The parameter SHOULD be used for preventing   cross-site request forgery as described in Section 10.12.

The client directs the resource owner to the constructed URI using an   HTTP redirection response, or by other means available to it via the

user-agent.

For example, the client directs the user-agent to make the following   HTTP request using TLS (with extra line breaks for display purposes

only):

```
 GET /authorize?response_type=token&client_id=s6BhdRkqt3&state=xyz
&redirect_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb HTTP/1.1
 Host: server.example.com
```

The authorization server validates the request to ensure that all   required parameters are present and valid. The authorization server   MUST verify that the redirection URI to which it

```
will redirect the
   access token matches a redirection URI registered by the client as   described in Section
3.1.2.
   If the request is valid, the authorization server authenticates the   resource owner and
obtains an authorization decision (by asking the   resource owner or by establishing approval
via other means).
   When a decision is established, the authorization server directs the   user-agent to the
provided client redirection URI using an HTTP   redirection response, or by other means
available to it via the
   user-agent.
```

Revision #1
Created Wed, Mar 25, 2020 10:52 PM by □□□
Updated Wed, Mar 25, 2020 10:53 PM by □□□