

# 4.1.2. 授权响应(4.1.2. Authorization Response)

## 4.1.2. 授权响应

Content-Type: application/x-www-form-urlencoded" 重定向URI

- code 授权码，由系统自动生成，长度不超过100个字符。
- state 重定向URI中的state参数，用于防止CSRF攻击。

HTTP 302 Found

HTTP/1.1 302 FoundLocation: https://client.example.com/cb?code=Splxl0BeZQQYbYS6WxSbIA&state=xyz

重定向URI

## 4.1.2. Authorization Response

If the resource owner grants the access request, the authorization server issues an authorization code and delivers it to the client by adding the following parameters to the query component of the redirection URI using the "application/x-www-form-urlencoded" format, per Appendix B:

code REQUIRED. The authorization code generated by the authorization server. The authorization code MUST expire shortly after it is issued to mitigate the risk of leaks. A maximum authorization code lifetime of 10 minutes is RECOMMENDED. The client MUST NOT use the authorization code

RFC 6749

OAuth 2.0

October 2012

more than once. If an authorization code is used more than once, the authorization server MUST deny the request and SHOULD revoke (when possible) all tokens previously issued based on that authorization code. The authorization code is bound to

the client identifier and redirection URI.

state

REQUIRED if the "state" parameter was present in the client authorization request. The exact value received from the client.

For example, the authorization server redirects the user-agent by sending the following HTTP response:

HTTP/1.1 302 Found Location:

[https://client.example.com/cb?code=Splxl0BeZQQYbYS6WxSbIA  
&state=xyz](https://client.example.com/cb?code=Splxl0BeZQQYbYS6WxSbIA&state=xyz)

The client MUST ignore unrecognized response parameters. The authorization code string size is left undefined by this specification. The client should avoid making assumptions about code

value sizes. The authorization server SHOULD document the size of any value it issues.

Revision #1

Created Wed, Mar 25, 2020 10:46 PM by [ ]

Updated Wed, Mar 25, 2020 10:47 PM by [ ]