10.5. 授权码(10.5. Authorization Codes)

10.5. 授权码

授权码的传输应该建立在安全通道上，客户端应该要求在它的重定向URI上使用TLS，若该URI指示了一个网络资源。由于授权码由用户代理重定向传输，它们可能潜在地通过用户代理历史记录和HTTP参照标头被泄露

授权码明以纯文本承载凭据使用，用于验证在授权服务器许可权限的资源所有者就是返回到客户端完成此过程的相同的资源所有者。因此，如果客户端依赖于授权码作为它自己的资源所有者身份验证，客户端重定向端点必须要求使用T

授权码必须是短暂的且是单用户的。如果授权服务器观察到多次以授权码交换访问令牌的尝试，授权服务器应该试图吊销所有基于泄露的授权码而颁发的访问令牌。如果客户端可以进行身份验证，授权服务器必须验证客户端身份，并确保授权码颁发给了同一个客户端。

10.5. Authorization Codes

```
   The transmission of authorization codes SHOULD be made over a secure   channel, and the
client SHOULD require the use of TLS with its   redirection URI if the URI identifies a network
resource.  Since
   authorization codes are transmitted via user-agent redirections, they   could potentially be
disclosed through user-agent history and HTTP
   referrer headers.
   Authorization codes operate as plaintext bearer credentials, used to   verify that the
resource owner who granted authorization at the   authorization server is the same resource
owner returning to the
   client to complete the process.  Therefore, if the client relies on   the authorization code
for its own resource owner authentication, the   client redirection endpoint MUST require the
use of TLS.
   Authorization codes MUST be short lived and single-use.  If the   authorization server
observes multiple attempts to exchange an   authorization code for an access token, the
authorization server
   SHOULD attempt to revoke all access tokens already granted based on   the compromised
authorization code.
```

```
   If the client can be authenticated, the authorization servers MUST   authenticate the client
and ensure that the authorization code was   issued to the same client.
```

Revision #1
Created Wed, Mar 25, 2020 11:21 PM by □□□
Updated Wed, Mar 25, 2020 11:21 PM by □□□