10.3. [illegible](10.3. Access Tokens

10.3. [illegible]

[illegible] RFC28181.6[illegible]TLS [illegible]

[illegible]URI[illegible]

[illegible]

10.3. Access Tokens

```
   Access token credentials (as well as any confidential access token   attributes) MUST be kept
confidential in transit and storage, and   only shared among the authorization server, the
resource servers the
   access token is valid for, and the client to whom the access token is   issued.  Access token
credentials MUST only be transmitted using TLS   as described in Section 1.6 with server
authentication as defined by
   [RFC2818].
   When using the implicit grant type, the access token is transmitted   in the URI fragment,
which can expose it to unauthorized parties.
   The authorization server MUST ensure that access tokens cannot be   generated, modified, or
guessed to produce valid access tokens by
   unauthorized parties.
   The client SHOULD request access tokens with the minimal scope   necessary.  The
authorization server SHOULD take the client identity   into account when choosing how to honor
the requested scope and MAY
   issue an access token with less rights than requested.
   This specification does not provide any methods for the resource   server to ensure that an
access token presented to it by a given
   client was issued to that client by the authorization server.
```

Revision #1
Created Wed, Mar 25, 2020 11:19 PM by [illegible]
Updated Wed, Mar 25, 2020 11:20 PM by