3.1.2.1. [illegible](3.1.2.1. Endp

Request Confidentiality)

3.1.2.1. [illegible]

[illegible]“code”[illegible]“token”[illegible]1.6[illegible]TLS[illegible]TLS[illegible]TLS[illegible]TLS[illegible]TLS[illegible]

[illegible]

3.1.2.1. Endpoint Request Confidentiality

```
   The redirection endpoint SHOULD require the use of TLS as described   in Section 1.6 when the requested response type is "code" or "token",   or when the redirection request will result in the transmission of
   sensitive credentials over an open network.  This specification does   not mandate the use of TLS because at the time of this writing,   requiring clients to deploy TLS is a significant hurdle for many
   client developers.  If TLS is not available, the authorization server   SHOULD warn the resource owner about the insecure endpoint prior to   redirection (e.g., display a message during the authorization
   request).
   Lack of transport-layer security can have a severe impact on the   security of the client and the protected resources it is authorized   to access.  The use of transport-layer security is particularly
   critical when the authorization process is used as a form of   delegated end-user authentication by the client (e.g., third-party   sign-in service).
```

Revision #1
Created Wed, Mar 25, 2020 10:35 PM by [illegible]
Updated Wed, Mar 25, 2020 10:36 PM by [illegible]