目前APP大都支持长登录，就是用户登录一次后，如果用户没有主动注销、清除APP缓存数据或卸载APP，就在一段时间内或一直保持登录状态。一般情况下，有以下三种方式：

利用Token实现

APP登录成功后，服务器以某种方式，如随机生成N位的字符串作为Token，同时设置一个有效期，存储到服务器中，并返回Token给APP。
后续APP发送请求时，都要带上该Token，每次服务器端收到请求时，都要验证Token和有效期，Token数值对且在有效期内，服务器返回所需要的结果，否则返回错误信息，提示用户重新登录。
(这种方式目前使用的最多)

利用Cookie实现

APP登录成功后，服务器创建一个包含session_id和Expires两个属性值的Cookie，存储在服务器中，并发送给APP。
后续APP发送请求时，都要带上一个包含此session_id的Cookie，每次服务器端收到请求时，都要验证session_id和有效期，session_id数值对且在有效期内，服务器返回所需要的结果，否则返回错误信息，提示用户重新登录。
(这种方式类似浏览器的认证方式)

利用用户名和密码实现

APP登录成功后，APP每次发送请求时，都把用户名和密码也发送给服务器，服务器每次收到请求都要验证用户名和密码。如果用户没有登录或注销了，发送请求时，就不把用户名和密码发送给服务器。