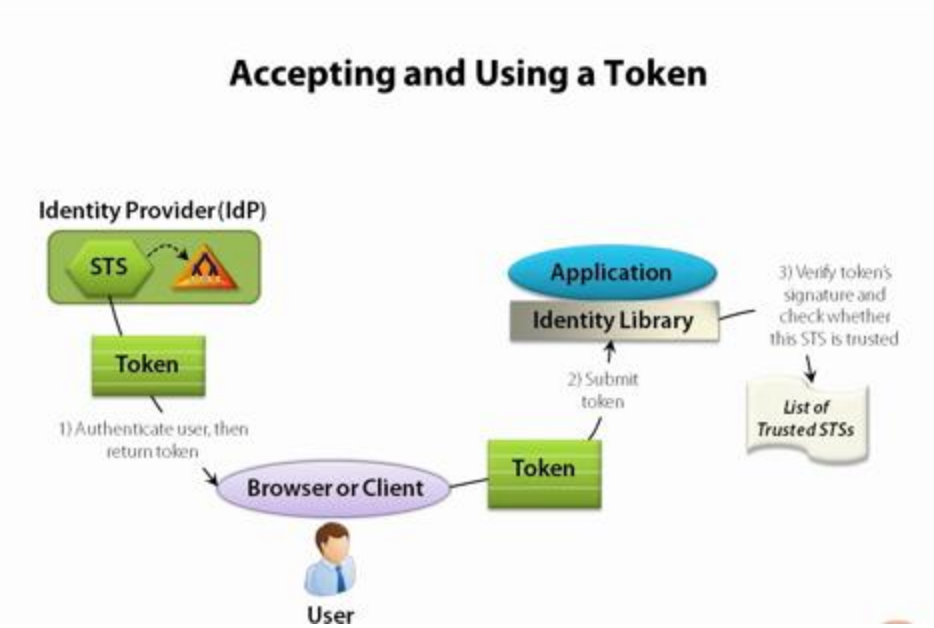

To make sure this is clear lets walk through how a user gets a token.

1. The process begins when a user or browser requests a token from some STS. That STS is provided by an Identity provider commonly called IdP.
2. Once it receives the request that STS must authenticate the user, that is, it must make the user prove it is who it really claims to be.
3. How does it do this?
   One approach is to let the user provide a user name and password. If the user is who they say they are then the STS begins constructing the token the user has asked for. Tokens contain claims - information about this user. So the STS must find that information from somewhere.
4. To do this it relies on an Account/ attribute store. One common example of this store is Active Directory. Active Directory is not the only choice there are numerous other ways to build STSs that don't require using AD or any AD service.
5. Lets imagine that the STS gets what it needs to construct the claims in this token.
6. It then sends the token back to the user after digitally signing it.
7. The user now has a tool that he or she can use to access applications
8. The user now has a token that he can send to an application he would like to access
   The application needs to process that token, this means that the App developer potentially has to write the code to do this but since all types of applications would like to do this, it actually makes sense to provide a common identity libray that does this on behalf of the application other wise it is too dificult to write the code for each application.

   The library does several things, it check the clients' signature to make sure it was not tampered with, and it can also now figure out which IDP issued this token.

The application need not necessarily accept this token. Instead it maintains a list of trusted STSs and trusted IdPs. Which of these is it going to accept tokens from? Lets assume that the STS checks the list and decides that the STS that issued this token is one it trusts (that is it believes that the claims in this token are true), it can now use those claims anyway its likes.