Session 是一种HTTP存储机制，目的是为无状态的HTTP提供的持久机制。所谓 Session 认证只是简单的把 User 信息存储到 Session 里，因为 SID 的不可预测性，暂且认为是安全的。这是一种认证手段。   
  
而 Token ，如果指的是 OAuth Token 或类似的机制的话，提供的是 认证 和 授权 ，认证是针对用户，授权是针对 App 。其目的是让 某App 有权利访问 某用户 的信息。这里的 Token 是唯一的。不可以转移到其它 App 上，也不可以转到其它 用户 上。   
  
转过来说 Session 。Session 只提供一种简单的认证，即有此 SID ，即认为有此 User 的全部权利。是需要严格保密的，这个数据应该只保存在站方，不应该共享给其它网站或者第三方App。   
  
所以简单来说，如果你的用户数据可能需要和第三方共享，或者允许第三方调用 API 接口，用 Token 。   
如果永远只是自己的网站，自己的 App ，用什么就无所谓了