为与“伪”单点登录(为解决遗留系统问题，而采用

自动模拟表单登录的方式达到单点登录)区分开。我们

采用统一认证的单点登录方式．在统一认证单点登录

系统中，应用系统与认证中心建立信息关系，若认证

中心认为用户具有合法身份，那么应用系统就相信认

证中心的“判断”，承认该用户具有合法身份．在这种

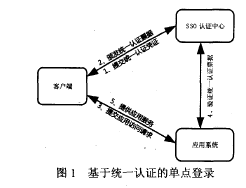
机制中，一旦用户在单点登录组件上登录成功，以后

再访问该单点登录框架中集成的任何应用时，就不需

要进行显示或隐式的登录操作．也就是说，对应用系

统而言，以前发生在其上的认证过程不再发生了，在

会话有效期结束前，只需登录一次．



统一认证单点登录如图1所示，其执行过程如下：

1)在用户使用单点登录组件之前，管理员需要向

单点登录组件注册所有应用系统的相关信息：用户向

认证中心提供认证凭证，证明其合法身份；

2)若用户通过主认证，单点登录组件将根据相关

规则为其生成一个用于联系该用户和被请求应用的票

据，并将该票据发送给用户：

3)当用户申请登录某个应用程序时，票据将随着

用户的请求一起转发至应用程序：

4)应用系统收到带有票据的用户请求之后，为了

验证票据是否有效，将利用票据与单点登录组件进行

一次交互，单点登录组件进行验证之后再向应用返回

肯定或否定的答案．

5)应用根据票据验证结果决定是否向用户返回资

源．

统一认证单点登录过程，类似第三方认证过程．

这种解决方案的优点是：用户信息维护成本较低：用

户认证信息的安全性较高；可以实现如单点登出，用

户集中管理等其他功能