? 统一认证

2. 第三方身份认证 跳过整个系统后台，支持微软域AD服务器的用户身份认证（采用这种方式，角色、授权等管理均失效）

AD所有的用户账户的维护是否手动维护？认证后的用户账户如何与平台用户关联？

3. 基于PKI技术构建的证书身份认证 为制定后台用户配置一个证书或者证书密钥U-key，此功能登陆实现预留，后台管理中，用户字段添加证书选择和是否证书认证字段。

PKI需要在服务器配置CA和IIS配置SSL（https），其中的服务器证书如果不是CA机构颁发的证书，在访问网站的时候会有“该站点不受信任”的提示页面。

4. 基于LDAP技术构建的身份认证 目前不适合用在教师、学生和一般用户的管理系统中，功能待定。

LDAP是一种协议概念，ACTIVE DIRECTORY是MS基于LDAP的一种产品。和第2点是类似的。如果要支持AD登录，那么数据中心的用户（教师/学生/一般用户）必须添加一个字段用来匹配AD中的账户名。

5. 基于session与cookies的存活周期管理 增加session或者cookies的选项，用于制定系统级别的认证生存周期存活规范。切换需要重启服务器。

session存在于服务端，cookie存在于客户端。单点登录采用的方式是：用户登录，登录后的凭证在服务器端可以存在于（1.数据库 2.缓存），前者可靠，请选择是否存到数据库。客户端如果选择了记住密码，那么他的用户凭证将记在客户端cookie里，下次访问时，站点读凭证，看凭证是否有效（存在于数据库或缓存中）。 数据库和缓存会根据预定的时间清除到期的凭证。 对于现在在用的单点登录中，部分用户无删除cookie权限导致无法退出或更换用户的问题，解决方式是：不论用户的凭证存在于客户端还是服务端，读取凭证后，都先到服务器验证凭证的可用性，再根据凭证取用户；且分站只取1次cookie。

示例一： 用户A的凭证是000，那么在服务端会有（000-A）这样的记录，客户端会有000记录；时间到期后，服务端（000-A）记录被清空，客户端登录，认证000已经失效。

示例二： 用户A的凭证是000，那么在服务端会有（000-A）这样的记录，客户端会有000记录；此时用户退出，服务端清空（000-A），但客户端由于权限问题删不了cookie。 下次用户访问分站X，X首次取出客

户端的000验证，000在服务端失效，返回登录页面，登录后服务端新增（111-A），并把111返回给分站X。分站X根据111取用户A的信息。