业务系统统一身份认证对接规范

南京航空航天大学 · 信息化处（信息化技术中心）

2019年11月

目录

[一、适用范围 2](#_Toc24543739)

[二、用户认证信息要求 2](#_Toc24543740)

[三、系统登录方式要求 3](#_Toc24543741)

[1．只有校内用户的系统登录要求 3](#_Toc24543742)

[2．存在校外等非统一身份认证用户的系统登录要求 5](#_Toc24543743)

[3．管理员登录要求 5](#_Toc24543744)

[4．业务系统中不存在用户的登录处理要求 6](#_Toc24543745)

[四、业务系统用户注销的要求 6](#_Toc24543746)

[五、业务系统对接流程 7](#_Toc24543747)

[六、系统运行要求 7](#_Toc24543748)

统一身份认证系统是学校信息化基础支撑平台之一，为业务系统提供认证服务，用户不再需要记忆多套账号密码。为更好的提升用户使用体验，提高网络安全水平，保障学校各类业务系统与学校公共数据库、综合服务门户、统一身份认证等公共基础支撑平台有效稳定的对接、集成和数据交换，特制定本规范，供学校各类业务系统对接统一身份认证系统时参照执行。

一、适用范围

凡学校建设和使用，且系统用户包含全校（或部分）教职工或学生的各类业务系统，必须使用学校统一身份认证系统进行用户身份认证。如系统用户仅限于本单位内部，鼓励进行统一身份认证的对接，如不对接，须保证系统自有身份认证系统的安全性并落实实名制管理的要求。

二、用户认证信息要求

1.实行统一身份认证的业务系统，普通用户登录后只能使用工号或学号授权使用系统，不允许存在其它授权身份识别信息。

2.业务系统中师生的基本信息来源于学校的公共数据平台的推送，在业务系统中用户只允许查看业务相关的必要的个人基本信息，不允许提供修改个人信息的功能。如果用户个人信息有误，须按照学校公共数据平台的数据治理要求进行修改。

3.业务系统内不允许对统一身份认证用户提供用户密码修改功能。如系统已有该功能，则必须对统一身份认证用户屏蔽该功能。

4.业务系统只允许对超级管理员、校外用户、其他非学校统一身份认证用户提供单独的认证机制和个人信息、密码修改功能。

5.业务系统用户统一身份认证信息须与学校公共数据平台定时同步对接，不允许根据统一身份认证的返回结果自动生成。

三、系统登录方式要求

1．只有校内用户的系统登录要求

**方式一：通过“综合服务门户”中“应用系统”和“快捷入口”进入。**

第一步：登录综合服务门户（http://i.nuaa.edu.cn），系统会重定向到统一身份认证系统（图1），用户输入自己的统一认证账户登录。



图1：学校统一身份认证系统

第二步：通过综合服务门户首页中的“应用系统”登录相应系统或者通过“快捷入口”下链接进入（图2）。



图2：综合服务门户首页

**方式二：通过业务部门网站跳转链接进入。**

第一步：点击业务部门网站的系统导航按钮或者链接（以“计划采购一体化管理系统”为例，图3）。



图3：国资处网站

第二步：对于已经登录学校统一身份认证的用户，则直接进入到业务系统中；对于未登录学校统一身份认证的用户，将直接跳转到学校统一身份认证页面，输入工号/学号和统一身份认证密码登录。

第三步：统一身份认证完成登录后直接进入到业务系统中。

2．存在校外等非统一身份认证用户的系统登录要求

需要在网站上对用户类型进行区分，分别跳转到不同的登录页面。校内用户登录须直接跳转到学校统一身份认证页面，校外用户登录则进入到系统自有的认证页面（以学校“计划采购一体化管理系统”为例，图4、图5）。



图4：存在校外等其他用户的页面设计



图5：校外用户登录进入系统自有登录页面

3．管理员登录要求

**业务系统不允许在业务部门网站上体现管理员登录链接和地址**。系统管理员的密码，须符合至少中级密码强度要求（8～16个字符，且必须包含大写、小写、数字、符号中的两种，定期修改密码），杜绝出现弱密码问题。系统管理员（用户名非职工号、学号）的登录，由管理员自己收藏具体网址。同时，在管理员登录页面中禁止学校统一身份认证用户使用此页面登录，并在页面中做出说明（图6）。

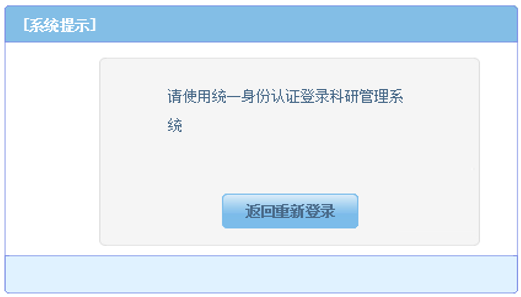


图6：学校师生通过此地址登录后会给出提示

4．业务系统中不存在用户的登录处理要求

用户登录该系统时，如用户不是该业务系统的合法用户，则业务系统须给出不能登录原因的友好提示，提示应包括为什么不能登录系统，该如何处理等内容（图7）。

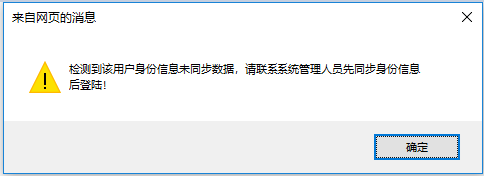


图7：系统针对不存在用户登录后的提示

用户点击确定后，可以关闭当前页面或跳转到其它页面。

四、业务系统用户注销的要求

所有与统一身份认证进行对接的业务系统，在退出或注销业务系统时，都应同时调用统一身份认证系统的注销地址，以注销统一身份认证，保证登录安全。业务系统注销后可以返回到统一身份认证系统的首页或者业务部门的网站首页，**不得返回业务系统自有的登录页面**。

五、业务系统对接流程

各业务系统在招标文件、合同及项目建设需求中须明确要满足统一身份认证的对接要求，在系统设计、开发阶段可提出统一身份认证对接申请，流程如下：

（1）业务系统主管部门的信息化联络员通过邮件（网上办事大厅对接申请流程上线后通过网上办事大厅申请）向信息化处提出统一身份认证的集成申请，申请信息中需明确系统的用途、使用对象、负责人及联系方式、建设厂商、厂商联系人及联系方式、系统的开发语言、域名等关键信息，申请邮箱为：xxhc@nuaa.edu.cn。

（2）信息化处对提交的系统对接申请进行审核。

（3）申请通过后，由业务系统承建商、信息化处（信息化技术中心）、业务部门共同讨论确定统一身份认证集成方案，业务系统承建商负责方案编制并提交给信息化处备案，然后由业务系统承建商具体实施并完成测试。

六、系统运行要求

新建设的业务系统，提交上线申请前须完成与学校统一身份认证系统的对接。不符合对接规范要求的业务系统，不予上线。

已经上线运行的业务系统，须按照本规范进行系统改造，直至符合要求。