**统一用户体系与系统单点登录系统**

**需求**

为了全面梳理医院信息系统用户管理体系,统一数据标准，整合服务内容，支撑医院统一用户的建设工作。以医院一体化HIS系统为核心，作为用户的枢纽，实现全院内数字化系统的用户注册、用户认证、用户登陆、账户授权、用户行为审计等服务的一体化。

以“人”为中心，打通用户在各个应用系统间个人信息管理、账户体系等内容，让使用者在不同应用系统中操作时，无需进行账号切换；整合面向个人的服务内容，实现个人信息维护，个人信息授权访问等功能，全面提升医院系统使用者的使用体验。在提升用户体验的同时，保障同一用户在不同的应用系统中身份的一致，解决幽灵账户、权限异常、越权行为等安全隐患，有效保护用户密码、身份信息和其他隐私数据安全。

**具体技术标准与功能**

**一 技术要求**

|  |  |
| --- | --- |
| 序号 | 技术要求 |
| 1 | 采用Token 认证机制 |
| 2 | 采用OAuth2.0授权许可机制协议 |
| 3 | 采用微服务架构 |
| 4 | 采用WebAPI开放标准协议 |
| 5 | 满足互联互通五级乙等及以上、电子病历六级及以上和智慧服务三级及以上评测标准。 |

**二 功能要求**

|  |  |
| --- | --- |
|  | 功能要求 |
| 接入应用系统管理 | 1 应用系统注册 | 注册接入系统的系统名称、系统地址、系统LOGO、用户类型、发布环境、应用系统类型、责任单位、接入状态等信息。注册成功后，自动生成该系统的AK、SK，该唯一标识和密钥，作为后续每个对接接口的必填输入参数。 |
| 2 应用系统访问视图 | 每个系统用户登录个人中心系统后，都能在个人中心首页看到用户自己可以使用的应用系统。有权限访问该系统，才能“进入”；有权限管理该系统，才能拥有“管理”权限；无权限访问和管理的系统不会看到。 |
| 3 应用系统的超级管理员设置 | 在每个接入系统的应用配置页面，应有“系统管理员”功能，关联系统中已有用户，作为本系统的超级管理员。系统管理员可以导入用户，导入后用户将有权限访问本系统。 |
| 4 应用系统与用户的关联 | 将所有接入系统的已归集用户信息进行融合操作；各个接入的系统与本系统所属的用户进行关联。 |
| 用户管理 | 用户管理功能 | 支持用户的失效、用户的注销、用户的实名认证、用户的预警、用户信息维护等功能。实现了用户与人员的关联，加强了对人员的访问控制、系统的安全防护。 |
| 认证与授权 | 认证与授权功能 | 用户名密码认证、CA认证。 |
| 日志审计 | 日志审计功能 | 具有用户登录日志（查询和查看接入系统用户通过，用户名密码登录，CA认证登录，其他系统免登、调用接口登录等方式的登录信息，实现安全审计功能）、系统访问量查询统计功能、用户量统计（按各接入系统、变动用户量（新增用户、变更用户、注销用户、到期用户）的维度，统计各维度截至目前的用户量和总计用户量）、日志统计分析（用统计表格、统计图表的形式分析系统访问量、用户变动量、访问峰值等）等功能。 |