四环医药集团统一身份管理平台培训手册

信息流程管理部 陈志富
2019.06

目录
CONTENT

随着企业的快速发展，各种业务系统和用户数量也在不断地增加，访问控制和信息安全问题愈见突出，原有分散的**“独立认证、独立授权、独立帐号管理”**的模式已经不能满足目前及未来企业信息化发展的要求，构建一个**完整统一、高效稳定、安全可靠**的集中身份认证和管理平台已经成为信息化建设的重要目标。

用户使用

多套账号密码

- 用户需设法记忆若干套系统的账号和密码；
- 每个系统都有密码更改周期，用户需更改多套系统账号密码；

多系统登录切换

- 用户需频繁登录切换系统，各系统账户独立无关联，无法无缝切换；

授权系统入口分散

- 用户无法全面了解自己已被授权系统，工作入口分散；

面临运营管理和用户使用上的问题

运营管理

人员信息孤岛，管理成本上升

- 各系统独立运营独立维护人员账户主数据信息，数据质量参差不齐，不共享不统一，维护难度大成本高；

系统功能重复，增加投入成本

- 公共功能重复开发，数据重复维护，增加系统建设成本投入；

存在信息安全风险，无法统一管控

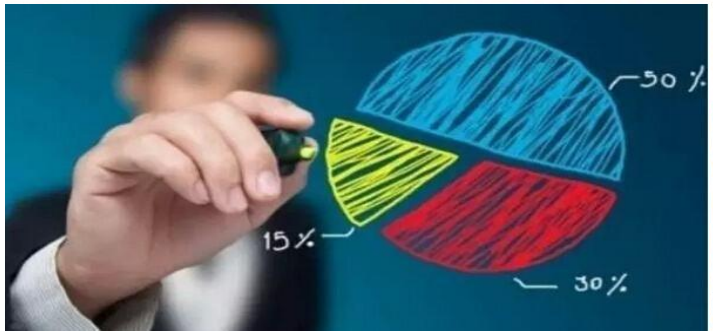
- 无法集中管理用户帐号并对其进行全生命周期管理，离职人员账户清理不及时存在信息泄露风险；

统一身份管理平台方案概述

平台建设目的

- 统一身份管理平台旨在达成多个系统之间身份数据的统一和身份认证的统一，使得用户只需要提供一次凭证就能在多个授权系统之间访问；
- 平台提供统一身份认证功能，用户无需记忆多套繁杂的用户名和密码，并在此基础上实现对身份数据的审计与账号的全生命周期管理，提升系统安全性；

整合、容纳、共享、门户



平台定位

- 为四环医药集团**统一登录认证门户**网站，打通系统间人员身份数据孤岛，既有系统逐步接入， 实现人员账户信息的全生命周期管理；
- 未来四环医药集团新建信息化系统登录账号统一为同一套账号和密码，实现单点登录，平台提供**接入规范和实施标准指导**。

平台建设思路

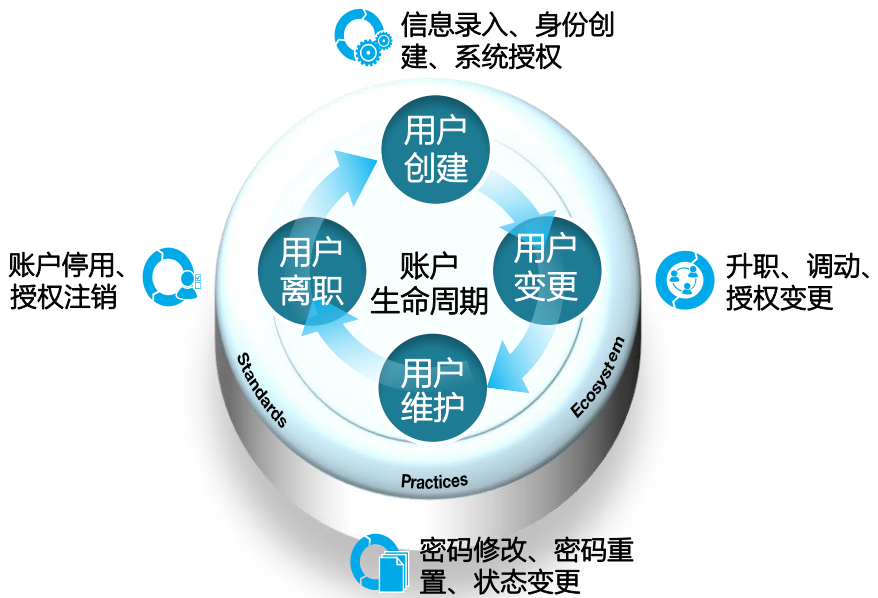
- 集团为每位员工提供唯一的账户和密码，统一身份管理平台通过员工入职、离职等状态联动进行账户的开通及关闭，及时回收与清理离职员工的系统权限，实现对账户的全生命周期管理；
- 通过统一的账户安全策略，实现对用户系统访问行为的统一管理，消除安全隐患；

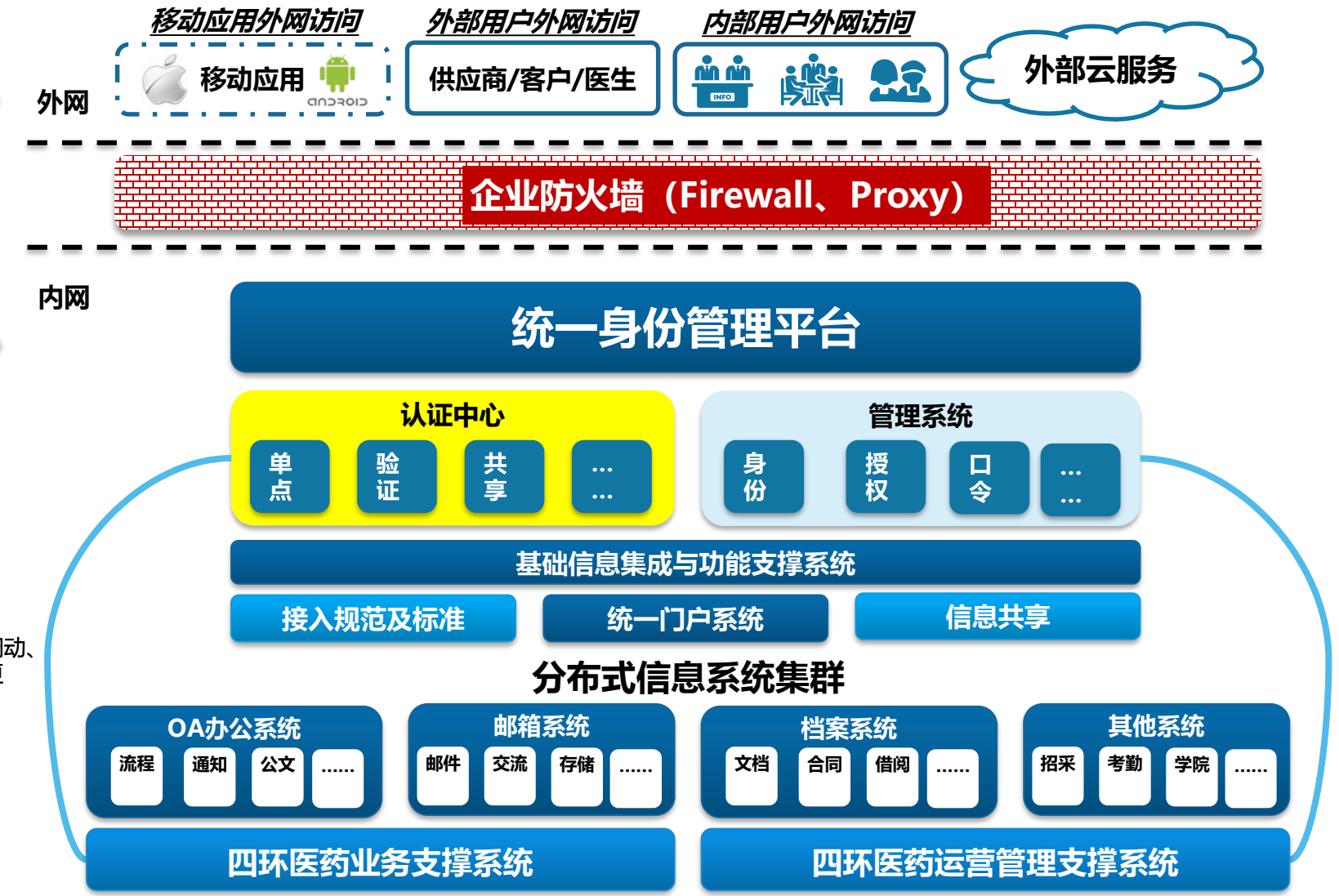
统一身份管理平台架构蓝图

1 面向全集团多终端的统一登录门户与身份认证支持平台

提供全集团内外部用户授权资源访问的统一门户，提供信息共享与接入标准规范。

2 人员账号信息全生命周期管理平台





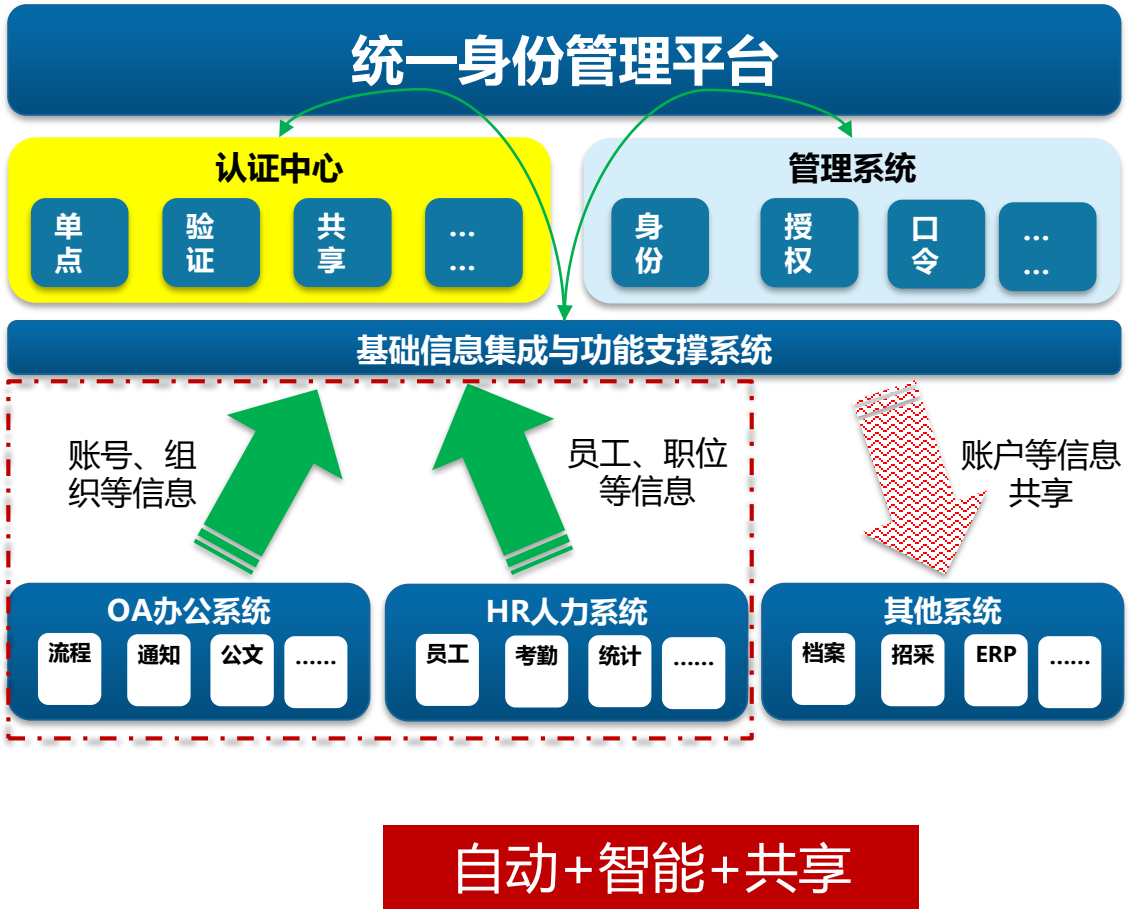
统一身份管理平台架构蓝图-人员账号信息全生命周期管理

I. 员工账号信息来源于HR和OA系统，且全集团**唯一**；

II. 当员工**入职**，平台基础信息集成子系统自动将员工相关信息同步至平台认证中心，完成**账户创建与开通**；

III. 当员工**离职**，由HR发起账户禁用，该账号状态信息将自动同步至平台；

IV. 账户**禁用**生效后，该账户将**无法登陆平台**，挂载其下的所有应用系统将**自动禁止使用**；
※ 当禁用的账户恢复启用时，原挂载的资源将一并启用，也可单独授权。



统一身份管理平台价值与收益

有效规避信息系统安全风险

以集团HR/OA管理系统为可信数据源，实现账户全生命周期管理，消除用户离职而未能及时关闭账户的信息安全隐患。

提高用户身份管理成效

通过统一账户名与密码、统一身份安全策略，与各相关信息系统有机结合，实现众多信息系统中的用户身份、账户属性、用户行为、账户全生命周期的集约化管理，提高用户身份管理成效。

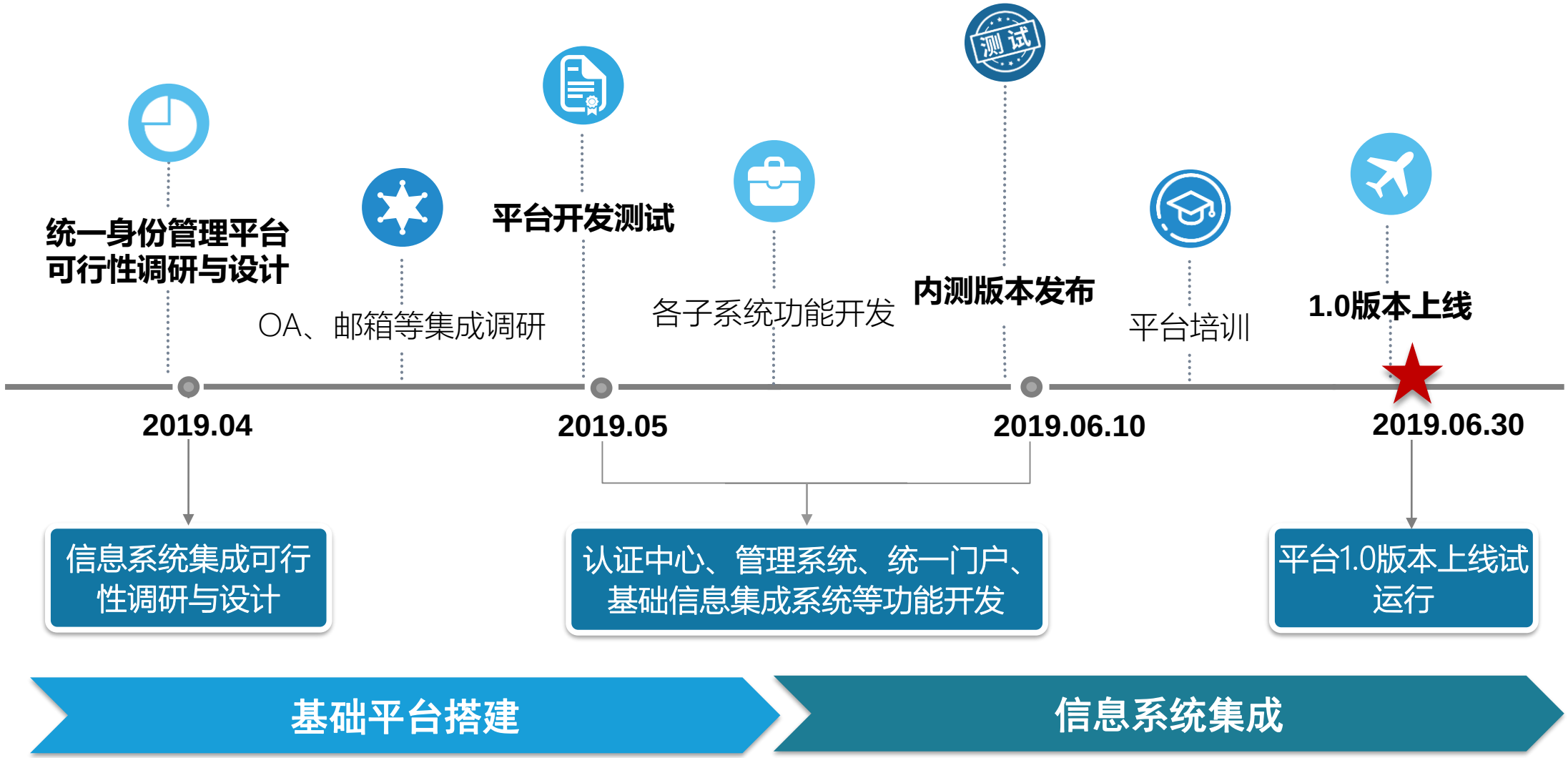
提升用户体验

实现跨信息系统单点访问，用户在同一浏览器只需输入一次账户名和密码即可访问其权限范围内接入了统一身份管理平台单点功能的所有信息系统。

降低系统开发和管理成本

账户数据集中管理能够有效减少各业务系统的重复数据存储、重复功能开发，极大降低 IT 管理成本。

统一身份管理平台整体计划



目录
CONTENT

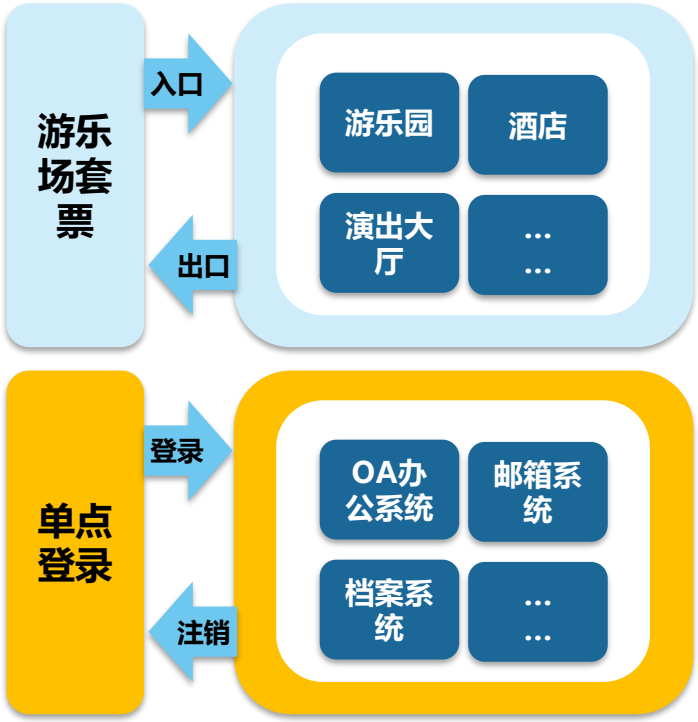
单点登录原理与应用简介

什么是单点登录

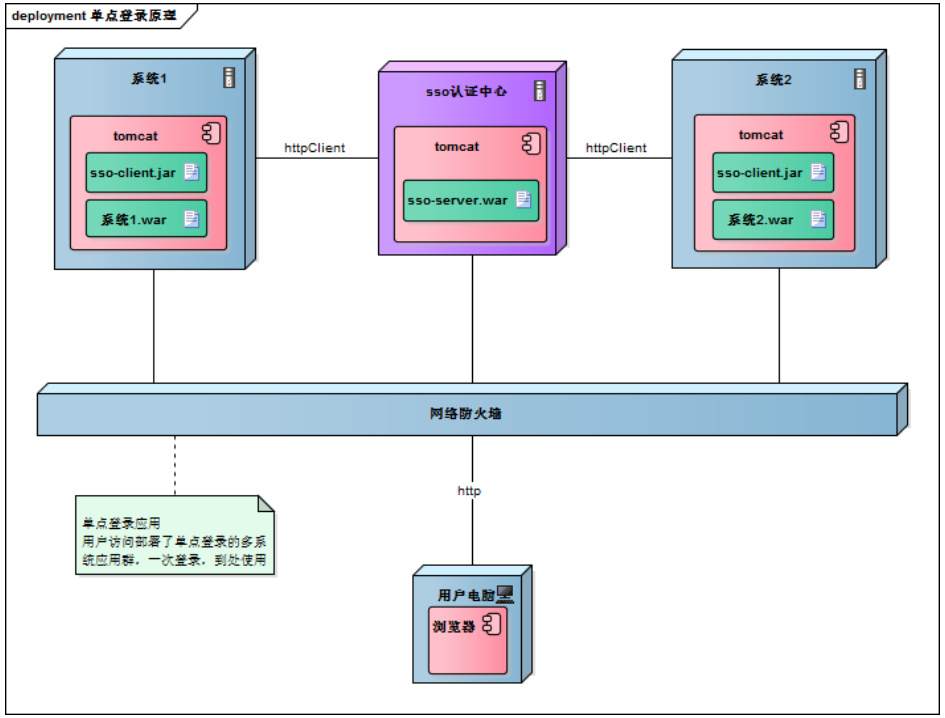
单点登录（Single Sign On），简称为 SSO，是目前比较流行的企业业务整合的解决方案之一。SSO的定义是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统。包括单点登录与单点注销两部分，**一次登录全网通行，一次注销全网注销**。

单点登录的实现原理

用户访问某系统受保护资源时，如果该用户尚未登录，则自动重定向到SSO的认证中心要求用户进行登录操作；用户登录成功后发放全局票据并跳转到用户请求的系统资源，系统从SSO认证中心获取认证用户信息，允许本系统资源的访问。



- ✓ **访问服务**：SSO客户端发送请求访问应用系统提供的服务资源。
- ✓ **定向认证**：SSO客户端会重定向用户请求到SSO认证中心。
- ✓ **用户认证**：用户身份认证。
- ✓ **发放票据**：SSO认证中心会产生一个随机的Service Ticket。
- ✓ **验证票据**：SSO认证中心验证票据Service Ticket的合法性，验证通过后，允许客户端访问服务。
- ✓ **传输用户信息**：SSO认证中心验证票据通过后，传输用户认证结果信息给客户端。
- ✓ **用户注销**：SSO认证中心销毁令牌与会话信息，客户端注销用户。



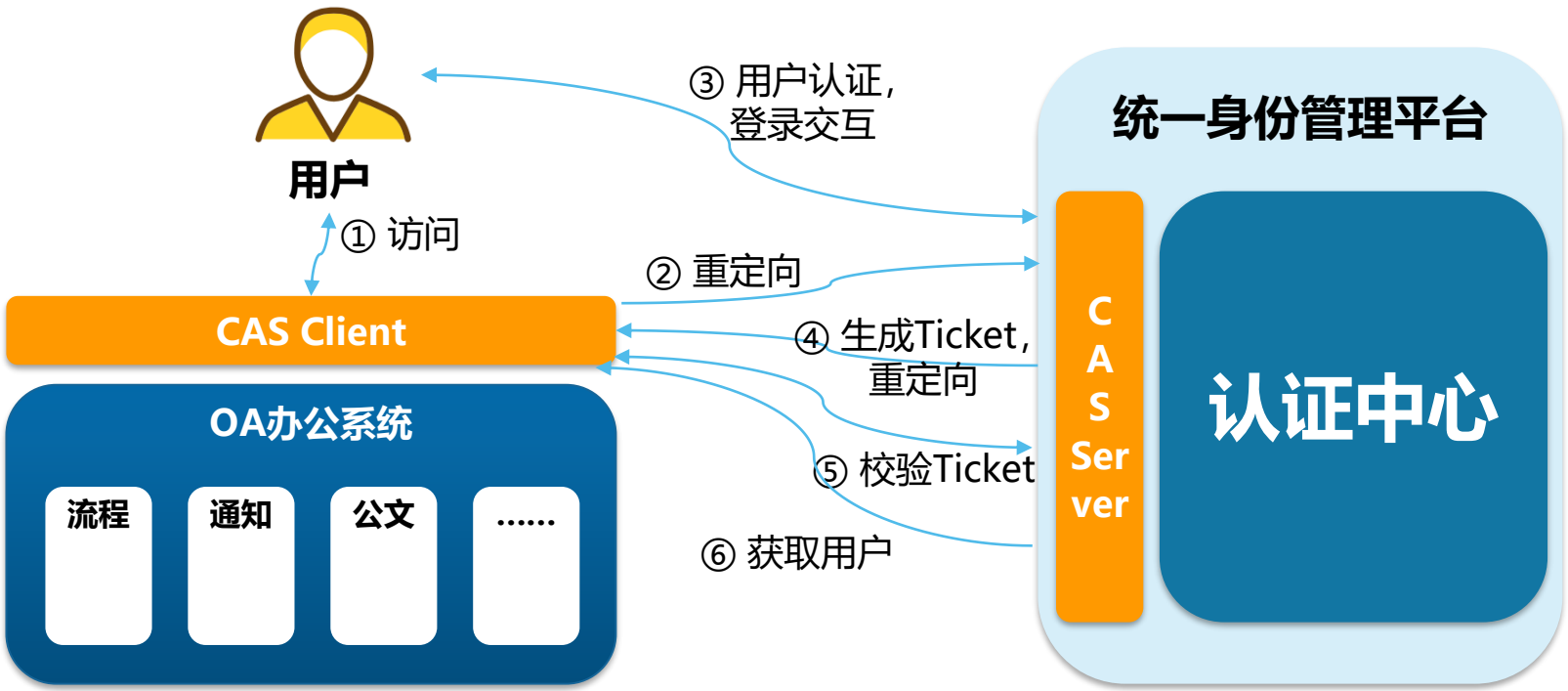
统一身份管理平台单点登录方案介绍

平台采用的单点登录方案

CAS（Central Authentication Service）是耶鲁大学发起的一个企业级的、开源的项目，旨在为 Web 应用系统提供一种可靠的单点登录解决方案。

统一身份管理平台单点登录结构体系包括 CAS Server 和 CAS Client 两部分。

- CAS Server 负责完成对用户的认证工作，需要独立部署，CAS Server 会处理用户名/密码等凭证（Credentials）。
- CAS Client 负责处理对客户端受保护资源的访问请求，需要对请求方进行身份认证时，重定向到 CAS Server 进行认证。（原则上，客户端应用不再接受任何的用户名密码等 Credentials）。**CAS Client 与受保护的客户端应用部署在一起，以 Filter 方式保护受保护的资源。**



- 用户访问网站，重定向到CAS Server端的登录页面，并且URL带有网站地址，便于认证成功后跳转，形如 https://sso.sihuanpharm.com/cas/login?service=http%3A%2F%2Fsoa.sihuanpharm.com%2F
- 用户在登陆页面输入用户名密码认证，认证成功后cas-server生成TGT，再用TGT生成一个ST。然后再重定向并返回ST和cookie(TGC)到浏览器。
- CAS客户端收到ST后再去CAS Server验证是否为自己签发，验证通过后显示页面信息。

当用户再访问其他接入CAS的系统时，因已有TGC，故而无需登录，但需要生成ST并重定向到客户端，校验后显示页面信息。

目录
CONTENT

统一身份管理平台使用手册

- 统一身份管理平台使用信息
- 集成前后系统使用变化说明
- 账户名命名规则与密码策略
- 确认个人基础与组织等相关信息
- 日常密码修改
- 自助查找账户名
- 自助重置密码

目录
CONTENT

统一身份管理平台常见问题与处理方法

- 常见问题与处理方法

目录
CONTENT

四环医药集团IT服务台

序号	姓名	电话	邮箱	备注
1	陈志富	18810605184	chenzhifu@sihuanpharm.com	平台整体架构
2	朱青	17600852286	zhuqing@sihuanpharm.com	平台日常运维
3	何莹	13810405033	heying@sihuanpharm.com	平台日常运维

THANK YOU!