# 基于 4A 管控的统一权限管理系统设计

陈 真 [1]
CHEN Zhen

**摘 要** 信息化方面的系统建设持续取得进步，信息技术被广泛应用到企业业务和管理工作中。国有企业数字化、网络化、智能化等方面得到飞速发展，持续增强竞争、创新、控制、影响、抗风险等能力。国家重视发展产业基础效能，提升产业链水平，信息化部门建设了大量信息系统，供业务及管理部门使用。在此过程中，存在建设系统数量多、开发商繁多、开发周期长、系统之间彼此独立形成信息孤岛的情形，不但很难适应企业对系统的快速响应，还会进一步影响高效的数字化转型进程。通过梳理和分析当前信息化系统建设过程中的影响因素，发现各系统重复的组织结构管理和差异的权限管理是影响信息系统建设的普适性问题。因此，通过调研和详细分析，基于 4A 平台解决方案建设统一权限安全管理平台，为所有系统提供统一组织和权限管理平台。

**关键词** 4A 管控；统一权限；权限管理；权限系统

doi：10.3969/j.issn.1672-9528.2024.08.007

## 0 引言

随着整个集团公司业务系统的不断发展，系统维护和使用人员不断增加，现阶段使用的账户管理方案无法满足安全维护的要求，更无法应对整个集团公司长期发展的态势。随着不同系统建设及用户增加，一方面会增加维护管理人员的工作，致使工作效率低下；另一方面对于不同业务系统，不能实施有效统一的安全策略管理。于是，遵循“事先取得授权，事中进行监控，事后统一审计”的规则进行监控管理权限全生命周期，在此基础上构建统一的权限安全管理平台，通过一种统一管理方案，对账户、授权、审计进行集中管理，从而对运维管理过程进行统一控制，使所有操作行为可审计。

## 1 系统设计原则

国外 IBM、SAP 等企业在技术理论、规范模型等方面开始较早探索，同时也产出了 RBAC、XACML 等不同方面的规范，这对不同类型信息系统的建设给予了极大的辅助建议。在国内的公司，无论国有企业还是民营企业，涉及 RBAC 权限管理方面的研究投入较多，特别是当下的互联网公司，在 RBAC 应用方面有较多的投入，由于各方企业在公司规划和管理方面的不同，导致现阶段国内的权限解决方案更偏向业务变化和复杂场景。在国家“十一五”规划开展至今，中央企业在大规模企业信息化下大力建设推进，信息化水平不断发展，在信息化方面的投资和支出也逐渐加大，持续助力企业信息化数字化转型工作。

截至目前，国内外企业信息化系统在授权管理方面主要有以下两种形式。

（1）基于 4A 管控的统一管理平台

1995 年，国际网络安全层面创造性提出了 4A 统一安全管理平台概念，将统一身份认证作为网络安全中最基础和重要的组成部分，即认证丨授权丨账户丨审计（Authentication 丨 Authorization 丨 Account 丨 Audit）。4A 被定义为网络安全方面的重要组成部分，身份认证在网络安全系统中起着不可替代的作用。

4A 统一安全管理平台是指能为平台用户提供符合萨班斯法案（SOX）要求的内控报表，主要涵盖用户账户管理、认证管理、授权管理和安全审计等四个大的方面，单点登录（SSO）等技术进行安全方面提高的功能，同时提供 4A 方向管理更高安全级别的功能。目前中国移动、中国联通、中国电信等大型运营商企业采用的方法是建立两级 4A 统一管理平台，以达到不同分公司内统一的账户管理和安全授权管理，管理方面的工作复杂度大幅降低，在统一监督下实现全面掌握企业安全状况，与萨班斯法案（SOX）提出的需求点一致。目前国内外大多企业会选择采用 4A 管理方案。由于 4A 平台管理方案比较规范，更适合信息化水平推进较为成熟的企业，但对特别复杂的组织架构和特别负责的权限设置使用灵活度较差，各子公司管理制度可能存在差异，如何实现整个集团统一的授权管理体系存在管理上的难题

1. 中国商飞民用飞机试飞中心 上海 201323

和技术实现上的复杂性。

为解决 4A 系统中各子系统接口改造难度大的问题，冯志杰等人 [1] 提出基于 SOA 架构的设计方案；徐骁麟等人 [2] 结合中移动网络空间安全需求，对 4A 平台的架构分层描述，对四大核心功能块进行归纳总结；马丽 [3] 根据甘肃联通基础网络安全运维要求，梳理业务需求、功能目标、覆盖范围和整体方案，提出一套联通 4A 平台设计方案。

（2）基于目录形式的统一身份认证管理平台

通过一套目录系统统一管控企业内部架构及权限资源。在华北电网，通过对异构统一账号管理平台（Oracle Idm）与目录服务（Novell Ldap）功能重构，实现打通门户协同功能，达到 SSO 单点登录。目录形式的解决方案实现简单，通过目录，统一管理用户账户、角色及授权，同时覆盖单点登录效果，技术实现简单，用户操作简单。其主要缺点是无法实现统一认证和授权，无法进行对应的安全审计等，对于复杂组织结构支撑薄弱，对管理人员要求较高。随着接入系统不断增加，管理投入也需要不断增加。一个基于 LDAP 目录服务的集成各种应用系统的访问控制方案，能够实现用户容易管理的访问 [4]。

通过上面两种管控形式，一些企业实现了部分组织机构的统一授权管理，基本能满足信息化的管控需求，但随着不同企业对信息化推进不断提高需求，期望进行统一资源（机构、人员）管理和授权管理、审计管理、安全方面提高等，上述两种模式并不能满足需求。同时，带来管理复杂度提高、人力资源浪费、授权风险等问题。因此，建立一套与企业现行组织架构契合、使用方便、能够适用不同场景的授权管理平台，是企业信息化进程中的必然趋势。

综上所述，现行的人员 / 组织管理和授权管理方式的解决方案已然不能适用大多数企业的发展，研发和建设统一权限安全管理平台是非常必要的，以适应现在复杂的使用场景。

## 2 系统功能模块介绍

### 2.1 认证管理模块

认证管理功能的着重点在于主 / 从账户的统一认证，即如何通过主 / 从账户实现统一认证，集中统一认证功能控制，同时保证通过主 / 从账户最终对权限资源访问的安全性。

（1）认证方式需求

认证管理需求指主 / 从账户如何通过单点登录进行认证。在安全性方面，可以采用不同的认证业务选用各异的认证形式，统一管理平台系统中所有的认证方式。对于主 / 从账户的认证，可以选择静态密码认证，或不同的强认证策略，常见的有令牌、短信、生物信息等方式。

（2）单点登录需求

用户使用主 / 从账户通过接入方系统单点登录到统一权限安全管理平台进行认证，认证过程通过统一单点登录接口完成。

### 2.2 授权管理模块

作为统一权限安全管理平台的核心功能组件，授权管理的主要功能是满足不同的第三方接入系统涉及权限的统一授权，这里的授权指的是实现系统权限分配到用户的过程。授权管理是指不同管理员在统一权限安全管理平台上将权限赋给主 / 从账户的过程，得到授权人员在个人权限范围内使用权限操作。授权管理过程包括主账户与组织机构、用户组、身份关联管理，角色、权限、接入方资源管理。

授权管理阶段，管理员管理权限与角色，不同角色会关联配置不同的权限集，其次再将不同的角色关联不同主账户，从而完成对用户的完整授权过程，相应的授权模型如图 1 所示。

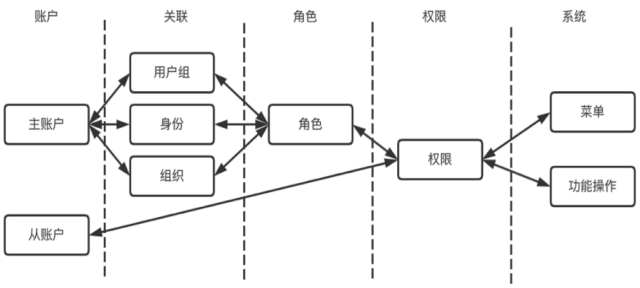


图 1 授权模型图

首先，通过接入系统管理员将第三方接入系统的菜单资源和权限资源分配给权限。在统一权限安全管理平台中资源主要分为两大类：菜单资源、功能操作资源。一个权限可以设定为访问不同菜单和使用不同功能操作。

其次，通过平台管理员或介入方系统管理员将权限配置给角色，一个角色拥有不同的操作权限。

再次，通过平台管理员或介入方系统管理员将角色赋给组织结构、用户组、身份，任何一个组织结构、用户组、身份都可以拥有不同的角色。

最后，将主账户关联到不同组织机构、用户组和用户身份。通过平台管理员或接入方系统管理员将从账户配置给主账户，也就是建立从账户与主账户之间的关联关系。同时，可以通过主账户用户将从账户直接关联到主账户已获得权限上。

### 2.3 账户管理模块

账户管理需求中纳入管理的账户，包含在整个公司业务运营过程中能适应所有系统的全部账户，主要分为主账户和从账户，由统一权限安全管理平台管理员维护。账户管理模

块的功能包括主账户管理、主账户配置及从账户管理。

首先，主账户管理功能涵盖以下方面。

（1）对于主账户全生命周期管理：如对新增、删除、修改、查找、是否可用等。

（2）对主账户属性的管理：对主账户基本属性管理，如主账户账号、主账户密码、主账户关联人员 ID；还涉及主账户状态：包括正常、锁定、删除三种状态；还有主账户按照其实际工作情况关联配置，主要包括配置主账户关联的人员、组织机构、业务身份、用户组、相关的从账户。

（3）主账户状态管理：主账户根据实际使用中的常见情况，至少应该设置正常、锁定、逻辑性删除三种状态。其中，正常指允许此主账户正常配置后登录接入当前统一权限安全管理平台的所有第三方系统，根据分配的权限访问第三方资源；锁定指暂时关闭此主账户登录访问权限操作，可以通过解锁操作将其恢复正常，常用于当多次尝试登录输入错误密码，告警系统提示非法登入或违规操作等异常情况，暂时切断主账户使用，解锁功能应该由主系统管理员操作，或授权于部分子系统管理员操作；逻辑性删除指永久停用此主账户登录统一权限安全管理平台或访问权限资源，无法通过其他方式恢复正常，主要场景是对应员工从单位离职，或第三方供应商服务期终止。由于主账户特性，为后续审计，主账户不能物理删除。

（4）主账户时效管理：应支持对于长期未使用的主账户自动锁定，防止出现主账户长期未登录后续却被用于攻击或者其他违法操作，通过时间阈值控制主账户自动锁定。

其次，从账户是由主账户持有者开设拥有部分权限的分账户，从账户由主账户持有人分配给第三方人员，从账户使用人可以通过从账户形式实现主账户人员的部分权限功能。

从账户作为授权体系中一个独特的存在，是为了解决实际过程中用户的授权，通常来说，收取按操作应该由具有授权权限的管理员进行统一授权处理，管理所有用户的权限也是统一集中授权，后续也由相应管理员对用户权限关联进行增删改查。而从账户是解决实际过程中，已有权限的用户临时授权相同功能权限给不同处理人员，由直接权限分配人员管理和对分配的从账户负责。对从账户管理功能涵盖以下方面。

（1）对于从账户全生命周期管理：对从账户的新增、编辑、删除、可用性。

（2）从账户状态管理：管理从账户的正常、锁定、逻辑删除三种状态。

（3）从账户时效管理：主账户可以根据实际情况控制从账户的过期时间。

2.4 审计管理模块

审计管理模块主要包括对审计数据进行标准化、对过程中产生的数据进行处理、对生成的数据进行清洗操作、对使用人员操作行为分析等，主要功能包括以下几方面。

（1）待审计数据的标准化操作：首先，如何进行数据合法性校验，审计规范对进行校验的数据的管控；其次，如何进行日志完整性、原始性校验；再次，映射日志字段，将日志数据处理为标准化字段；最后，将日志数据进行补全操作，补全日志映射后的字段。

（2）中间生成数据的处理操作：主要是筛选日志内容、分析业务场景。筛选日志内容主要是在标准化后的日志中，根据日志筛选规则按照信息筛选；分析业务场景是根据具体审计业务特殊场景分析规则，分析出日志中的异常问题，作为审计展示专题。

（3）数据采集：主要是收集保存接入系统的日志行为。本系统设计的采集数据范围包括不同接入系统的账户数据、授权数据，认证数据、登录登出日志，管理类日志等。

（4）分析用户行为：选取主 / 从账户一个时间区域内的日志数据，分析识别数据，使用归并、分拣、聚类等方法进行建模，将构建的模型的条件设定访问 IP、触发时间范围、触发周期、行为结果分析等。

图 2 为审计管理用例图。

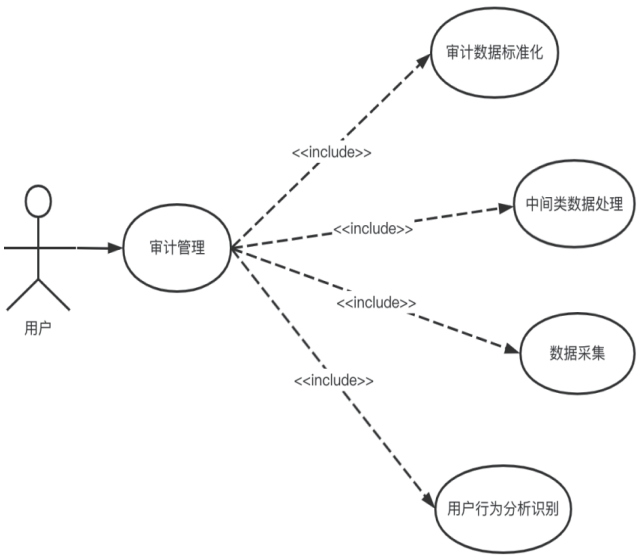


图 2 审计管理用例图

**3 系统设计与实现**

分析前面整体业务需要，采购分层设计模式，对统一权限安全管理平台进行总体框架分层架构，设计分层为集中展示层、核心功能实现层、集中数据层、适配接口层、统一资源层以及第三方安全组件六个部分。集中展示层是集中展示

核心功能层的实现结果；核心功能层基于业务功能设计数据统一层的数据；集中数据层管理平台中不同类型数据库里的资源；接口适配层是提供接口给核心功能层和集中统一数据层；第三方安全组件主要对核心功能层的功能进行安全方面的补充，例如采用动态口令、短信口令、生物特征等方式进行认证等。

对于已建成的系统，采用了不同技术的多套生产与业务系统，需要集中管控所有用户账号，李茂鑫 [5] 设计完成了一套 4A 平台，实现统一集中的管理、认证、授权和审计功能；郭威 [6] 针对在企业认证管理过程中产生的数据访问安全性与便携性发生的矛盾，构建企业身份、权限、认证、审计 4 大体系，设计并实现了一种具有多重认证为统一认证中的增强型功能的 4A 系统；杨雪莲 [7] 将第三方系统与集中化人力平台进行联动，实现与用户数据同步，建设内蒙古移动公司统一用户平台，将账户管理朝着集中化、独立化、中心化方向推进。

统一权限安全管理平台的核心框架包括集中展示层、核心功能层以及接口适配层，是完成平台的账号管理、认证，进行可视化操作的主要方面。结合集团公司的实际情况需求及业务内容，对统一权限安全管理平台进行分层设计，图 3 为总体框架分层图。

对平台中主要基础子功能进行设计与实现，涵盖资源、授权、认证、审计、策略等五个管理功能子模块，其总体结构设计图如图 4 所示。

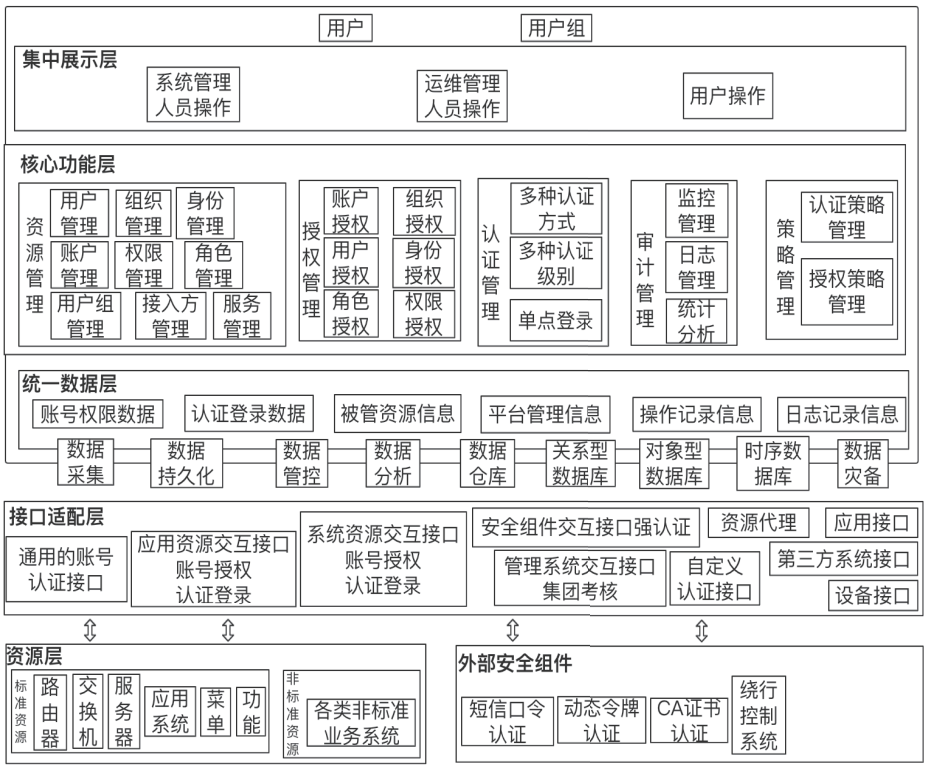


图 3 总体框架分层图

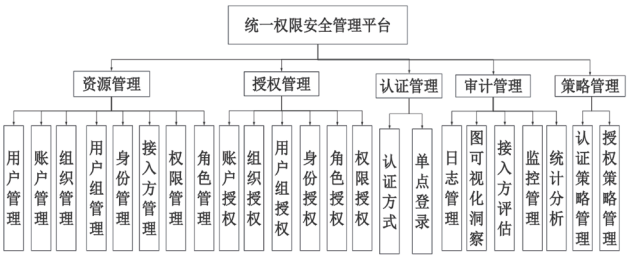


图 4 总体结构设计图

资源、认证和授权管理主要是管理平台内资源，以及资源之间的授权、认证。资源管理是管控平台内的主从账户资源，维护主从账户的属性。认证管理功能是对平台中资源的访问等操作进行认证操作，实现安全合法地进行资源访问。授权管理功能主要是管控平台中使用人员的权限范围限定，缩小授权用户访问操作的范围。

审计管理功能涵盖抽取、清洗、分析等操作平台内登录登出及操作日志。抽取日志是为了对主 / 从账户的记录数据实现进行管理和持久化存储。标准化处理日志数据后，根据统一策略功能中管理配置的规则，实现采用不同的算法处理当前选取的日志数据进行分析识别操作，以此发现可能存在的审计方面问题，确保平台内的安全，并且能够为审计出来的责任追踪提供作证。

## 4 数据库设计

统一权限安全管理平台账户管理模块包括主账户管理和从账户管理，主要包括主 / 从账户的增加、删除、编辑、查询等操作，为统一权限安全管理平台内所有的账户进行有效的管理。

在账户管理模块中的数据库设计图如图 5 所示，其中用户主账户表 CUserMainAccount 和从账户属性表 CUserFollowAccount 是最核心的数据库表，一个主账户对应关联若干从账户，以下详细说明数据表的设计。首先，CUserMainAccount 表管理是扩展主账户属性，实现平台系统对主账户属性变化的需求。主账户的关联属性包括登录账号、用户密码、关联用户、失效期、账号状态和允许使用 IP 集等。其中，允许使用 IP 集指的就是限制登录使用此主账户的 IP 地址。

角色关联模块数据库设计图如图 6 所示。CRole 为角色属性表，如果该当前角色授予主

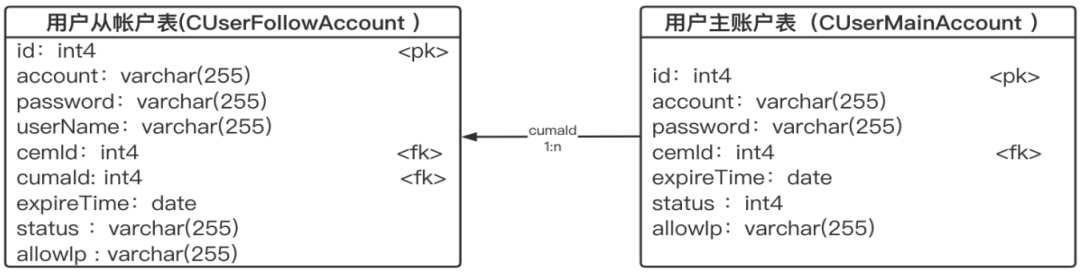


图 5 账户管理模块的数据库设计图

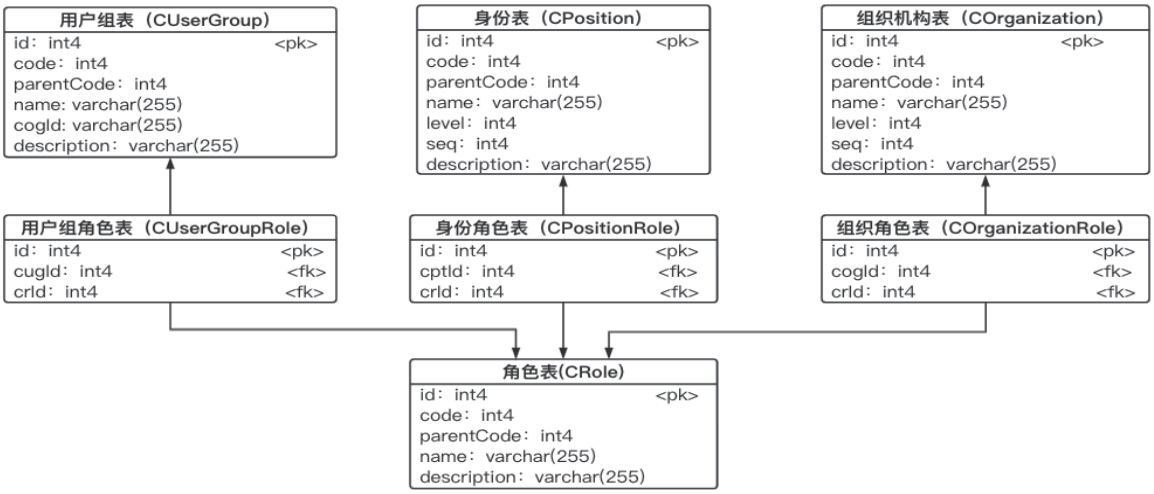


图 6 角色关联模块数据库设计图

体是组织机构，则为当前组织所有成员赋予角色。关联表 COrganizationRole 即为组织机构与角色关联表，如果该当前角色授予主体是用户组，则为当前用户组成员赋予角色，关联表 CUserGroupRole 即为用户组与角色关联表；如果该当前角色授予主体是身份，则为具有当前身份成员赋予角色，关联表 CPositionRole 即为身份与角色关联表。通常情况下，同一角色可以关联多个不同组织机构，可以关联多个用户组，可以关联多个身份。

## 5 结语

在当前信息化发展趋势和单位实际工作需要的共同作用下，4A 平台的应用价值日益凸显。部署 4A 平台不但整合了当前整个集团各中心日益庞大的各支撑系统，更为整个集团安全管控提供了集中式管理方案，减少集团对内部可能产生的威胁。结合当前信息化工作中的实际情况，在 4A 平台基础上扩展统一权限安全管理平台，作为对适应工作业务的 4A 平台的补充完善。对本平台进行编码实现，并对平台进行功能测试，同时上线试用维护。在测试过程中，通过黑盒测试法，实现相关测试用例。平台上线运营后，权限敏感数据的查询使用明显减少，有效减少了滥用权限的风险，提高了管理部门整体资源统一管理效率，满足当前使用部门的需求。

**参考文献：**

[1] 冯志杰 , 檀鹏 . 基于 SOA 架构的业务支撑网 4A 系统设计 [C]// 中国通信学会信息通信网络技术委员会 2009 年年会论文集 . 北京 : 中国通信学会信息通信网络技术委员会 , 2009: 162-166.

[2] 徐骁麟 , 穆琰博 , 宋菲 , 等 .4A 统一安全管理平台关键技术分析与评估 [J]. 电信网技术 ,2016(12):21-27.

[3] 马丽 . 甘肃联通 4A 统一安全管理平台的设计 [D]. 兰州 : 兰州交通大学 , 2019.

[4] 郑岚 , 陈奇 . 基于 LDAP 的统一访问控制系统的设计与实现 [J]. 计算机工程与设计 ,2005(7):1865-1867+1885.

[5] 李茂鑫 . 大型企业多套已建系统集中账号管控（4A）平台设计与实现 [J]. 中国新通信 ,2019,21(15):98-99.

[6] 郭威 . 企业级信息管理系统认证统一管理的设计与实现 [J]. 南方能源建设 ,2015,2(S1):234-238.

[7] 杨雪莲 . 运营商基于统一用户的账号管理平台实现 [J]. 数字传媒研究 ,2021,38(7):59-63.

**【作者简介】**

陈真（1988—），男，湖北黄冈人，硕士研究生，研究方向：信息系统、数据挖掘、商务智能。

（收稿日期：2024-05-16）