统一身份认证技术在企业信息化系统中的应用研究

闵晓霜，董　岩，王　皓，刘　红，刘雪飞，杨　跃，李奉原
（中国电子信息产业集团有限公司第六研究所，北京 100083）

摘　要： 针对企业信息化建设过程中面临的应用系统集成、用户身份管理等问题，基于4A统一安全管理规范，并结合企业多元化集成需求，提出统一身份认证与单点登录解决方案，建立统一身份管理平台。对系统功能进行分析与设计，并着重探讨基于Token的身份认证机制以及单点登录关键技术，提出多元化集成的单点登录方案，采用Spring Security实现JWT认证和授权。该系统可实现信息系统统一、高效、安全的用户身份管理，方便新应用系统的集成。

关键词： 统一身份认证；单点登录；Token；权限管理
中图分类号： TP393　　**文献标识码：** A　　DOI：10.16157/j.issn.0258-7998.212089

中文引用格式： 闵晓霜，董岩，王皓，等. 统一身份认证技术在企业信息化系统中的应用研究[J].电子技术应用，2022，48(9)：103-107，113.
英文引用格式： Min Xiaoshuang，Dong Yan，Wang Hao，et al. Research on the application of unified identity authentication technology in enterprise information system[J]. Application of Electronic Technique，2022，48(9)：103-107，113.

Research on the application of unified identity authentication technology in enterprise information system

Min Xiaoshuang，Dong Yan，Wang Hao，Liu Hong，Liu Xuefei，Yang Yue，Li Fengyuan
（The Sixth Research Institute of China Electronics Corporation，Beijing 100083，China）

Abstract： Aiming at the problems of application system integration and user identity management in the process of enterprise informatization，based on 4A unified security management standard and combined with the diversified integration needs of enterprises，this paper puts forward a unified identity authentication and single sign-on solution，and establishes a unified identity management platform. This paper analyzes and designs the system functions，focuses on the identity authentication mechanism based on Token and the key technology of single sign-on，puts forward a diversified and integrated single sign on scheme，and uses Spring Security to realize JWT authentication and authorization. The system can realize the unified，efficient and secure user identity management of the information system and facilitate the integration of new application systems.

Key words： unified identity authentication；single sign on(SSO)；Token；authority management

0 引言

随着信息化水平的提高，企业信息化程度逐步深入，为了保障管理与业务的高效运作，可能会进行组织架构调整、岗位人员优化、业务服务升级等，也陆续会有新的信息化系统上线。例如，目前在中国航油智慧加油系统建立了覆盖总部与各地区干线机场的统一多集群架构，总部中心集群部署了基础数据管理、业务数据汇集、中心数据分发、综合态势分析等应用系统，各地干线机场业务集群部署了基础信息管理、任务调度、综合监控、地图保障、加油作业等应用系统，随着加油前端与总部建立信息通道，加油调度及终端作业实现电子化，系统将进一步融合大数据、云计算、GIS、AI等，优化内部管理和扩展外部服务，构建新的应用系统，为各类用户提供相对应的信息化服务。

由于众多系统相互独立，且开发时间、开发商、技术架构等存在差异，这对信息管理人员以及用户都造成了身份信息管理的挑战。对于信息管理人员，要依靠低效的手动操作来支撑员工在各个应用系统中的密码重置、身份注册/注销等繁重却非常重要的身份管理工作；对于使用人员，则要记住多个应用系统的账号密码，分别登录各应用系统，这为用户日常工作造成了诸多不便。尤其是随着应用系统逐渐增多，出错的几率以及受到非法截获与破坏的可能性也会增大，安全性则会相应降低[1-2]。针对这种情况，统一身份认证、单点登录等概念应运而生，并不断地被应用到企业信息系统中[3-4]。

统一身份认证将各账户及认证方式进行统一与整合，面对多个应用系统，用户只认证一次，通过后就可以对任何有权限的其他应用系统进行访问，这就实现了单

点登录[5]。用户登录到一个门户界面，可以进入有权限的其他业务系统，解决了企业员工日常频繁登录各系统的烦恼，避免了忘记密码需要信息管理人员重置密码的困扰。建立健全的身份管理体系也有助于对用户访问权限、应用权限进行统一集中管控，对企业资源进行有效整合，保障并促进产业链中各角色之间的正确互通及高效合作。

1 统一身份管理系统功能分析

统一身份管理系统是对用户进行身份确认且分配使用权限的核心系统，实现对用户使用平台全生命周期管理，保障资源在权限范围内得到有效使用与管理[6]。针对未来种类繁多的应用系统，系统应支持多元化集成，对不同应用开发语言、认证源及认证协议实现全方位集成，统一认证，用户只需认证一次，平台内所有应用系统均可使用，无需进行重复认证。

4A(认证 Authentication、授权 Authorization、记账 Accounting、审计 Audit)统一安全管理规范涵盖统一的账号管理、认证管理、授权管理和安全审计，可有效解决企业对众多应用的统一访问、控制、授权的需求。基于该规范，并根据企业的现实需求，建立统一身份管理平台，实现以下功能：统一账号管理、统一身份认证、统一集中授权和透明操作审计，以及支持用户“一次登录，到处访问”的单点登录。

1.1 统一账号管理

实现统一身份认证，最核心的数据就是用户的身份信息，它是实现认证和访问控制的基础。系统应对平台内应用系统建立统一的用户账号体系，各应用系统再无须单独保有、维护这些账号信息。功能包含：用户账号的全生命周期管理、主从账号映射及关联管理功能。

1.2 统一身份认证

统一身份认证就是通过标识和鉴别用户身份，判断用户是否有权访问目标应用及功能，防止攻击者假冒合法用户来获取访问权限[7]。统一身份认证服务作为平台统一认证中心，为平台应用资源提供多种认证接口，实现平台用户的统一身份认证。支持账户密码登录、基于短信验证码的二次认证；支持基于 SAML、OAuth、OIDC、CAS 等标准认证协议。

1.3 集中授权管理

身份认证成功后，系统通过集中授权赋予用户进行应用、功能等的操作权限。系统提供对应用、功能及数据的访问权限设置，支持对用户的单独授权和对用户组的批量授权，支持通过角色绑定的方式进行授权。

1.4 用户操作审计

系统的每个使用者都该为自己的操作负责，每个操作都要留有记录，以便核查。系统需记录授权和非授权用户在系统中的用户行为，通过有效分析这些行为并直观呈现给安全管理员，可对用户审计提供有效依据。进一步地，通过一定量的数据积累，可形成一定规则，对行为异常的用户账号进行限制，并可在认证的时候实现主动防御、瞬间互动。

1.5 单点登录

单点登录(Single Sign On，SSO)作为统一认证后续功能，不仅提供一次登录平台即可打开平台内所有业务系统、减少认证流程、避免重复操作带来的安全隐患，还具有便捷办公、简化管理等诸多好处。系统应支持 PC 端应用资源，Pad、移动端单点登录，以及 API 接口单点登录 3 种方式。

2 统一身份认证与单点登录系统设计

2.1 总体设计

系统总体架构划分为 4 个层次：数据层、接口层、服务层和 UI 层，如图 1 所示。数据层采用 MySQL 关系数据库存储账号、权限等持久化数据，采用 Redis 缓存日志等；接口层为系统内外部提供面向数据的 API 接口，对外部系统以 API 的形式提供认证接口；服务层提供了统一账户、统一认证、集中授权以及操作审计的功能服务；UI 层提供用户操作的人机交互界面，包括认证入口、后台管理界面。

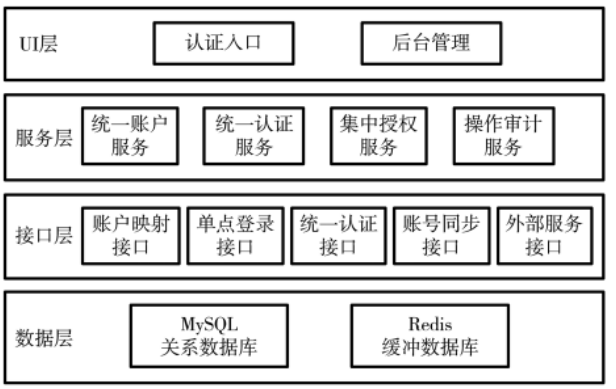

图 1 系统总体架构

系统采用基于 Restful/JSON 的前后端分离方式，无论是 B/S 还是原生 APP 应用类开发，一律通过 API 来调用后台服务器服务。前端 Web 界面架构基于响应式，支持不同设备分辨率，底层使用 Bootstrap 框架；使用JQuery 框架编写前面流程控制；采用流式布局，兼容各类操作系统及终端设备，还可兼容移动设备(如手机、iPad、PDA)。后端主要采用 Spring Boot、Spring MVC、J2EE、Spring Security 等一些成熟的开源技术，实现微服务体验，让每一个功能都能独立出来，便于扩展。

系统采用分布式部署，总部建立统一身份管理认证中心，同时各地区建设分认证中心各自进行用户与权限管理，分散总部平台认证压力。系统数据库采用两台 MySQL 都可读写、互为主备的设计，两台主库间做高可用，采用 keepalived 解决方案，使用 VIP(虚拟 IP)对外提供服务，当主库宕机时，备库就会接管 VIP 对外继续提供服务，保证了数据的高可用。系统的数据交互如图 2 所示。

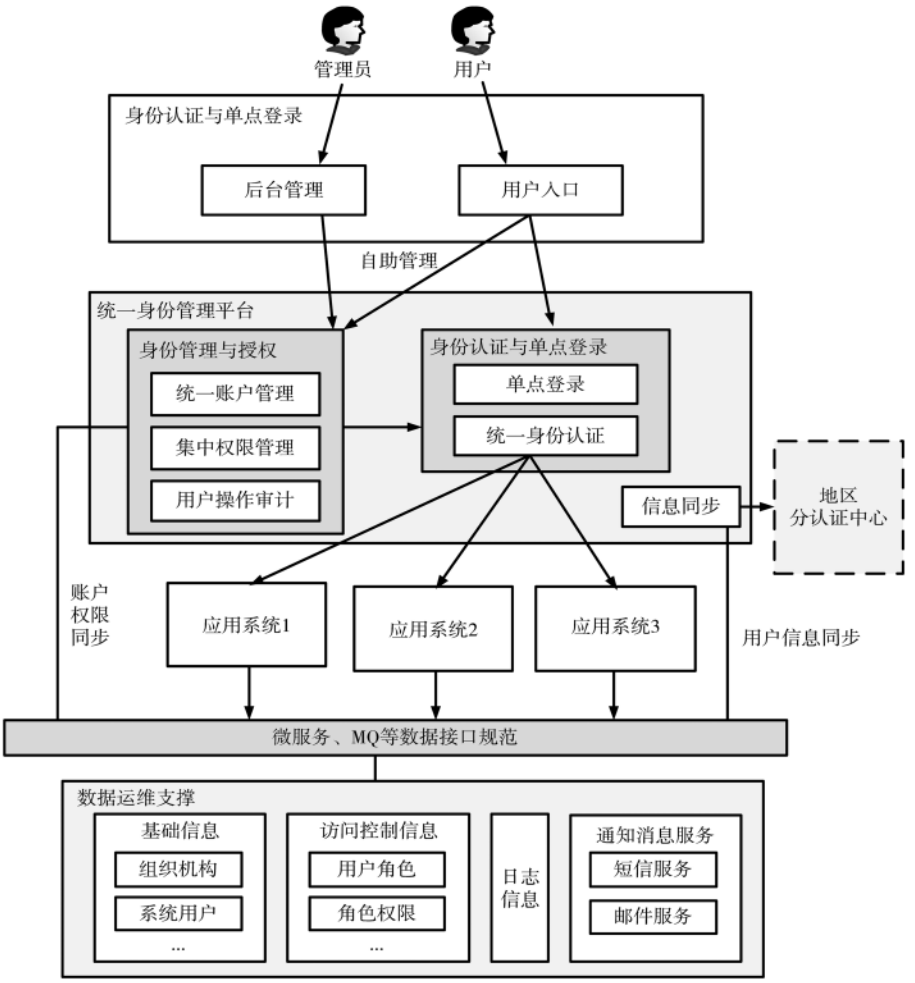

图 2　系统数据交互

2.2 主要功能设计

2.2.1 统一账号管理

(1)用户账号的全生命周期管理

系统对用户账号进行全生命周期管理，包括账号的创建、修改、删除以及对账号状态(停用、启用)的维护。出于安全考虑，除平台管理员或被授权用户外，不支持用户自行修改。用户账户详细信息包括：用户 ID、密码、姓名、性别、年龄、身份证号码(实名认证)、电话、岗位、所属地区、子公司等。密码进行加密存储，忘记密码则只能进行重置。

(2)账号管理机制

系统创建用户账号时，即创建一个唯一的系统主账号，该账号在各接入应用系统中通用，经授权的用户能登录并访问被授权的应用系统。系统也提供主从账号映射，用户可以通过账号关联配置，将自己在某个应用系统中的子账号映射到统一身份认证平台的主账号上，该方式适用于已有不可改造系统的接入。

(3)账号的批量管理

用户账号可单独管理，也可按照不同的组织方式进行集体管理。客观上，用户属于某个组织机构，处于某种岗位；主观上，管理员可对用户进行自定义分组管理，以分组 ID 标识不同的组。管理员可通过上述两种方式对用户进行批量管理，包括批量创建、修改、删除账号，批量停用、启用账户，批量重置密码以及批量授权等。

2.2.2 统一身份认证

系统为用户提供在各业务应用过程中的一次认证功能，支持不同域下业务应用的统一认证集成。通过集中资源管理、授权管理提供的集中身份信息和权限信息，能够消除用户信息系统的业务孤岛和数据孤岛。

平台用户进行实名认证，用户不具有自行注册、创建用户的功能。创建用户均需要平台管理员或者地区管理员在核实身份后创建，并绑定信任设备(如 PC、手机等)。用户提交身份信息与系统账号进行绑定，使用户 IT 身份信息与真实身份进行关联。

(1)二次身份认证

用户登录的身份验证支持基于动态短信的二次认证，流程如图 3 所示。

(2)基于 Token 的认证

身份认证模式主要有 2 种：Token 认证和 Session 认证。传统的 Session 认证是在服务端存储 Session，并向客

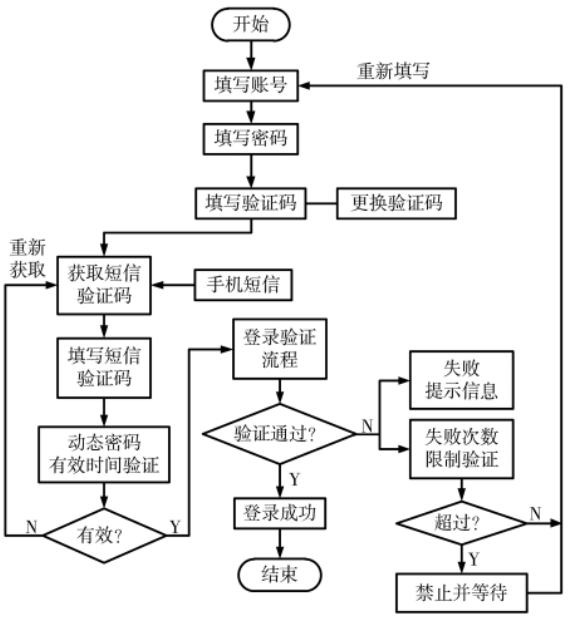

图 3 用户身份验证流程

户端返回带有 Session Id 的 Cookie，客户端每次请求带上 Cookie 到服务端校验，该方式存在诸多弊端[8]：用户并发访问量大或应用规模大时会占用大量服务器内存；难以横向扩展(跨域、跨服务共享资源)；Cookie 传输容易遭受 CSRF(跨站点请求伪造)攻击等。而基于 Token 的认证方式是无状态的，Token 只存储于客户端，客户端每次向服务端发送请求时都会携带 Token(由服务端签发)，服务端接收到 Token 时会进行验签，从而对用户身份以及 Token 有效性进行验证。

系统采用基于 Token 的认证方式，用 Token(JWT)来代替 Session 进行分布式的人员状态管理。用户认证成功后，获取用户的权限信息，并生成包含用户身份及权限等主要信息的 Token。Token 认证机制如图 4 所示，Token 存储在客户端且包含主要用户信息，服务端省去

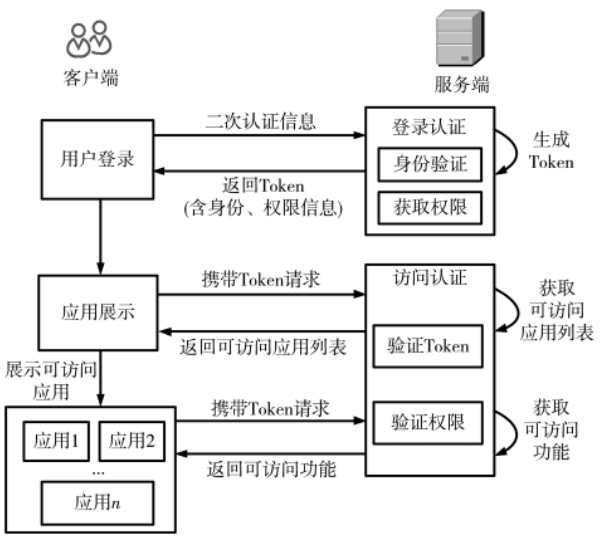

图 4 Token 身份验证机制

了存储会话及查询相关数据库的工作，有利于服务性能提升及横向扩展；由于不依赖 Cookie 机制，方便支持跨域访问，支持原生平台(iOS、Android 等)客户端。

2.2.3 集中授权管理

(1)角色与权限管理

可对系统角色进行增删改查等操作，内容包括：角色代码、角色名称等。

角色权限分配：可以对每个用户角色进行权限的分配，包括子系统的访问权限、关键功能和操作的执行权限、关键数据的访问权限或访问内容范围(如各分公司用户只能查看本单位相关数据)；可通过对角色(岗位)配置权限，再通过角色赋权给某个组织机构达到批量授权。

权限验证：对于系统关键操作及操作的数据内容，除在前端根据权限进行一定的限制和隐藏外，后台应进行权限验证，确保用户操作类型和操作的数据在其权限范围内，禁止非法或未授权的操作。

(2)权限管理策略

①分级管理

系统提供分级管理功能，使用户可以更明确、便捷地管理各个业务系统。管理员分为平台中心管理员、各地区管理员、平台中心安全管理员。

管理员在本平台可以进行下列工作：平台中心管理员(超级管理员)主要负责管理平台基本参数、用户和用户组的管理、应用管理、账户认证管理；各地区管理员主要负责管理辖区内各单位用户和用户组的管理；平台中心安全管理员可以根据 IP、时间段、用户名等进行安全审计，出现问题可以追溯。

②数据与业务功能的权限划分

这部分权限主要依据组织机构进行分级管理，组织机构可分为总公司、地区公司、(地区下属)子公司。

子公司用户具备对本单位相关数据的访问编辑权限，同时禁止对其他子公司的访问和编辑权限；地区分公司具备对本地区范围内子公司的相关数据的访问权限，不具备编辑权限，同时禁止对其他地区子公司的访问和编辑权限；总公司具备对全国所有子公司相关数据的访问权限，不具备编辑权限。

2.2.4 用户操作审计

(1)管理员审计功能

日志可以提供查询、备份等管理功能。各地区管理员可查询本地区日志，中心平台管理员可查询所有日志；安全审计员可以备份、删除日志；备份/删除日志操作时间有记录，备份/删除的记录不删除；可对备份提醒进行设置，管理员登录时系统将作出提醒。

(2)用户账户审计功能

系统支持检查某个用户一段时间内的使用情况，并且通过一系列安全策略建立起正常使用的模型。这样当

系统遭遇撞库等攻击时，能够及时自动做出响应，符合动态防御的原则：包括检查当前访问网络的用户数量；检查所有用户的访问高峰时间；发现试图登录无访问权限计算机的用户；查看任一用户的所有登录历史；当同一用户短时在不同地方登录，追踪分析用户的活动及安全状况；对用户设置关注的重点事件进行实时预警等。

3 统一身份认证关键技术

单点登录是实现用户一次登录，可直接进入其他应用系统的功能，主流的单点登录协议有 SAML、CAS、OAuth、OIDC 等[9]。

SAML 是基于 XML 的标准认证协议，定义了身份提供者 IDP(Identity Provider)和服务提供者 SP(Service Provider)之间如何采用加密和签名的方式来建立互信，从而交换用户身份信息[10]，SP 与 IDP 的信任关系需要提前将双方信息配置到对方，通过证书的方式建立。CAS(中央认证服务)是 Yale 大学发起的一个开源项目，包含 CAS Client 和 CAS Server，将 CAS Client 部署在客户端，以过滤器的方式对每个访问受保护资源的 Web 请求检查是否有 Service Ticket，有则到 CAS Server 进行验证，二者间的互信是通过接口调用方式实现的，不具备签名和加密机制。OAuth 一般指 OAuth2.0，是一种授权协议，解决的主要是第三方应用如何被授权访问资源服务器，由授权服务器负责授权，适合多种场景；OIDC(OpenID Connect)在 OAuth2.0 基础上扩展了认证的场景，是现在最流行的协议，引入了 id_token 概念表示资源拥有者的身份，标准化 id_token 的格式就是 JWT。SAML 和 OIDC 有相似之处，均通过签名和加密交换用户身份信息，SAML 是通过断言，OIDC 则是通过 id_token。

这些协议本质都是基于中心信任的机制，SP 和 IDP 通过互信来交换用户信息，只是交换的细节或概念有不同之处。

3.1 多元化集成的单点登录方案

依据单点登录实现方式，并为满足未来业务系统可扩展，认证协议划分为：已具备标准认证协议、提供接口可改造集成、C/S 架构系统、不可改造的 B/S 架构。针对这些情况，分别提供不同的单点登录解决方案。

(1)标准认证协议应用集成

针对支持上述标准认证协议的应用业务系统，提供标准模板，只需点击“添加应用”，进入后添加图标，填写应用名称、所需支持设备类型、登录地址等，便可完成集成工作。

(2)接口可改造应用集成

对于可改造(待开发中或支持二次开发)的应用使用票据 Token 方式，目标应用需配合调用身份认证中心提供的认证协议，根据应用业务系统认证机制确认是否需要 API 接口完成。这里采用 JWT，将 Token 解析能力植入应用系统，用户只需登录平台认证，认证成功后返回主 Token，登录业务系统均由系统本身自行解析，对平台性能损耗小、快捷。原理如图 5 所示，在应用端安装一个公钥(有插件)，当客户端发起请求时，身份认证服务端会返回一个通过私钥签名的 Token 给客户端；客户端的浏览器通过 302 跳转将 Token 传递给应用端，应用端通过公钥验证私钥的签名是否正确，如果正确就会登录应用，从而实现单点登录。

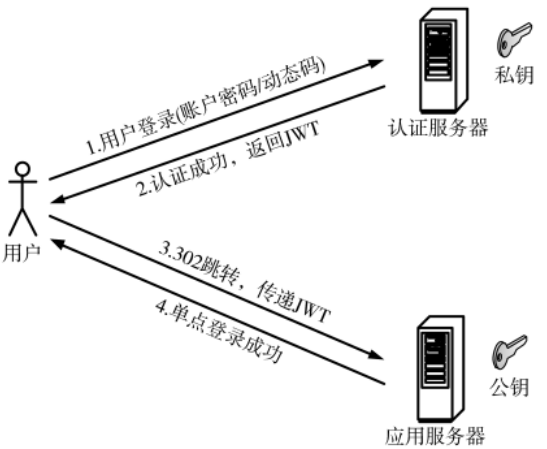

图 5 JWT 单点登录原理图

(3)C/S 架构系统

对于 C/S 架构的应用，采用 Kerberos 的代理方式进行集成。在客户端的统一认证门户点击一个 C/S 架构应用图标，客户端就会通知服务端；服务端通过一个 URI(唤醒 PC 端的代理)返回一个 Token(包含用户的账号密码)给客户端的代理，客户端的代理拿到 Token 之后，得知将要登录的是哪个应用；代理唤醒将要登录的应用，并将账号密码代填到应用；自动登录到应用的服务端，单点登录成功。

(4)不可改造的 B/S 架构系统

对于一些 B/S 架构应用系统不能停机或开发商不能配合改造的情况，采用表单代填模拟提交的方式。管理员为账号关联模板配置账号密码登录功能及用户认证参数；用户在系统中点击应用系统访问链接；平台自动提取从账号及密码(加密存储)，将账号及解密后的密码自动填充到目标应用的表单并提交，实现应用系统的登录。密码采用 AES 256 的加密方式。

3.2 JWT 认证授权

目前集成的都是新开发的系统，采用 JWT 进行认证授权。JWT 常用于在 IDP 和 SP 之间传递通过认证的用户身份信息，继而获取资源服务器中的资源[11]，由头部(header)、载荷(payload)和签名(signature)三部分组成。header 中描述了 signature 进行签名的算法，playload 用于携带用户信息，signature 对前两部分编码连接后，按照 header 中的算法加密签名。

(下转第 113 页)

[5] ROTHER C, KOLMOGOROV V, BLAKE A. Grabcut: interactive foreground extraction using iterated graph cuts[J]. ACM Transactions on Graphics, 2004, 23(3): 309-314.
[6] SHOTTON J, JOHNSON M, CIPOLLA R. Semantic text on forests for image categorization and segmentation[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2008: 1-8.
[7] LONG J, SHELHAMER E, DARRELL T. Fully convolutional networks for semantic segmentation[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2015: 3431-3440.
[8] CHEN L C, ZHU Y, PAPANDREOU G, et al. Encoder-decoder with atrous separable convolution for semantic image segmentation[C]//Computer Vision-ECCV 2018. Cham: Springer International Publishing, 2018: 833-851.
[9] CHEN L C, PAPANDREOU G, KOKKINOS I, et al. Semantic image segmentation with deep convolutional nets and fully connected CRFs[J]. Computer Science, 2014(4): 357-361.
[10] CHEN L C, PAPANDREOU G, KOKKINOS I, et al. DeepLab: semantic image segmentation with deep convolutional nets, atrous convolution, and fully connected CRFs[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2017, 40(4): 834-848.
[11] CHEN L C, PAPANDREOU G, SCHROFF F, et al. Rethinking atrous convolution for semantic image segmentation[J]. arXiv preprint arXiv: 1706.05587, 017.
[12] CHENG S, MA J, ZHANG S. Smoke detection and trend prediction method based on Deeplabv3+ and generative adversarial network[J]. Journal of Electronic Imaging, 2019, 28(3): 1-9.
[13] ZHANG K, LIU X, CHEN Y. Research on semantic segmentation of portraits based on improved DeepLabv3+[J]. IOP Conference Series Materials Science and Engineering, 2020, 806: 57-64.
[14] 杨坤山.基于深度学习的图像语义分割在三维重建系统中的应用与实时化[D].成都:电子科技大学, 2019.

(下转第 118 页)

(上接第 107 页)

Spring Security 框架为 Java 程序提供用户认证和用户授权功能,实现认证和校验身份的过滤器。系统在 Spring Boot 中整合 Spring Security,实现 JWT 认证机制。

JWT 传输携带许多用户信息,存储在客户端也有被窃取的危险,为保证 JWT 在认证与授权过程中的安全,采用以下方式:

(1)避免在 playload 中存放敏感信息;

(2)采用 HTTPS 协议,对 JWT 进行 SSL 数据加密传输,保证网络传输的机密性,防止中间人攻击;

(3)增强 JWT 时效性,减少 Token 被窃取盗用的可能性;

(4)在进行一些重要操作时,采用二次认证。

4 结论

随着企业信息化、智慧化的深入发展,将迎来信息化系统的爆发式增长,建设统一的身份管理平台,为新系统的推出建立标准、提供便利;本质中心化的信任机制,使得重要信息被纳入统一、集中管理,既提升了管理效率、保障了信息安全,又让应用系统能够专注于业务功能的实现。上述统一身份认证与单点登录系统方案在中航油智慧加油系统中得到了初步的应用,为信息化系统提供统一的用户管理与应用集成。本方案也为企业信息化系统的建设提供了参考。

参考文献

[1] 郑子秋,张卫东,刘宁,等.信息安全技术在企业 ERP 系统中的应用[J].科技创新与应用,2019(18):174-176.
[2] 李德兵,徐铁山,傅成兵.单点登录技术研究与应用[J].电子技术,2008(9):52-54.
[3] 李庆林.基于 WEB 的单点登录和权限管理技术研究与实现[D].北京:北京邮电大学,2017.
[4] 邱素华.基于身份认证技术的统一认证系统研究与实现[J].中国信息化,2021(12):59-60.
[5] 苏星晔,徐方南.统一身份认证技术研究[J].中国新通信,2015,17(2):58.
[6] 张伟健,曾世强,李培瑜.计算机网络安全威胁及对策[J].网络安全技术与应用,2017(9):1-2.
[7] 郭晓宇.统一认证授权技术浅析[J].网络安全和信息化,2022(1):24-26.
[8] 柳丽娜.浅淡 Session 机制与 Cookie 机制[J].电脑编程技巧与维护,2008(16):28-29.
[9] 李强.基于 CAS 和 OAuth 的统一认证授权系统设计[J].信息技术与网络安全,2021,40(6):83-88.
[10] 孙建华,王永生.基于 SAML 的统一身份认证技术的应用研究[J].信息技术,2015(9):63-66.
[11] 范展源,罗福强.JWT 认证技术及其在 WEB 中的应用[J].数字技术与应用,2016(2):114.

(收稿日期:2021-08-23)

作者简介:

闵晓霜(1987-),女,硕士,高级工程师,主要研究方向:信息系统软件、工控信息安全。

董岩(1976-),男,本科,工程师,主要研究方向:自动控制、智能信息处理及智能信息控制。

王皓(1973-),男,硕士,高级工程师,主要研究方向:智能工控系统及相关软硬件研发。

扫码下载电子文档

版权声明