

基于 RSA 与 MD5 签名的实名制微门户设计

洪丹丹, 罗军峰, 冯兴利, 徐 墨, 锁志海
(西安交通大学 数据与信息中心, 陕西 西安 710049)

摘 要: 以西安交通大学“互联网+”校园建设为背景, 解决传统微信应用服务单一且无法获取校内用户真实隐私数据问题, 设计并实现了基于 RSA 与 MD5 签名的实名制校园微门户系统. 提出在校内本地服务器上绑定微信用户的 OpenID 和校内统一身份认证系统的 CAS NetID 实现校内用户真实身份校验; 通过 RSA 加密与 MD5 数字签名实现用户敏感数据保护; 通过高度的校内系统集成, 实现微门户服务综合一站式. 应用结果显示, 移动用户通过微信客户端一键关注西安交通大学官方微信即可享受微门户综合服务; 通过实名绑定可获取基于用户真实校内身份与角色的敏感数据访问.

关键词: 微信; 一站式; 门户; 跨平台; 互联网+; 统一身份认证(CAS); RSA; MD5
中图分类号: TP391 **文献标识码:** A **文章编号:** 1000-7180(2016)09-0036-06

Design of a Real-name WeChat Portal Based on RSA and MD5 Signature

HONG Dan-dan, LUO Jun-feng, FENG Xing-li, XU Mo, SUO Zhi-hai
(Data and Information Center, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: To solve the problem that traditional WeChat applications can not provide comprehensive service for campus users based on their real identities or roles, a real-name WeChat portal with RSA and MD5 signatures was proposed to satisfy the mobile users in university campus. In this portal, a mechanism about binding OpenID of WeChat and NetID of CAS (Central Authentication System) was designed to realize the real-name identity authentication. To protect the private information, RSA and MD5 signatures were utilized during data transmission. To provide the comprehensive one-site services, all the campus service data used by portal were integrated based on the related campus systems. After testing and running this system in two months, the statistic reports show that it can provide comprehensive one-site service and cross-platform service to mobile users by the WeChat clients installed in their mobile devices. Meanwhile mobile users can also access the private data based on their identities after binding their WeChat accounts and CAS accounts.

Key words: WeChat; one site; portal; across platform; Internet Plus ; CAS (central authentication system); RSA; MD5

1 引言

利用微信公众号的跨平台、便捷消息响应等特性, 集成校园信息系统实现教育“互联网+”已成为近来学者研究热点. 校园信息门户作为校园信息化核心软件, 也需

要在“互联网+”时代以微信公众平台为媒介, 从软件形态、架构、服务模式等方面进行转型升级. 本文以西安交通大学微门户(微信公众号)建设经验为研究基础, 针对微信公众号无法实现校内用户真实身份与角色判定问题(精确到用户所在部门/学院, 教工/学生), 提出了将微信公众平台、校内统一身份认

证系统及校内业务系统进行三方集成,实现基于用户校内真实身份的一站式、跨平台、安全、可挖掘校园微门户并对敏感数据进行 RSA 加密与 MD5 签名。

本文首先分析了微门户建设目标并对微门户的整体功能模块、系统架构进行了设计;接着对微门户的消息响应机制进行了解析;然后对微门户中的实名制绑定及基于 RSA 与 MD5 签名的安全控制措施进行了实现;最后对微门户的敏感数据保护与跨平台支持进行了测试分析。

2 微门户建设目标

本文研究的实名制校园微门户建设目的是为用户提供一站式、跨平台、安全可靠的信息共享服务,同时为管理者提供基于用户真实身份的大数据服务。

一站式服务是指当用户一次登录后,即可享受多种类的综合业务服务(如一站式学生服务中心^[1],一站式电子政务^[2]等);跨平台服务是指帮助开发者实现一套代码多系统平台共享,减少开发者开发压力、降低项目建设成本,提高代码复用率;安全性服务保证用户避免传统数据安全威胁^[3]、云数据安全威胁和大数据安全威胁^[4];大数据服务是指充分利用一站式微门户的各种多源异构数据为学校管理者提供基于用户真实身份与行为的数据采集、数据融合及数据分析等工作(如获取用户的日常访问时间、服务类型、使用频次、地理位置坐标等要素,挖掘分析用户的学习行为、生活消费行为^[5-6],通过数据融合为学校领导层提供智慧决策辅助)。

3 微门户功能设计

由于本文的建设目标之一是为订阅了校园微门户公众账号的用户提供一站式综合校园信息化服务,因此其功能模块结构设计如图 1 所示。

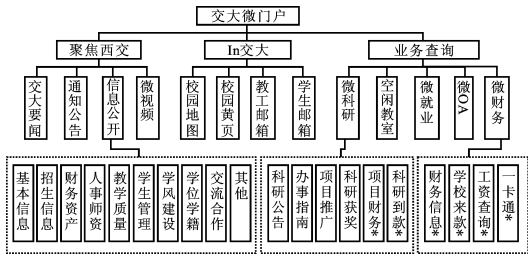


图 1 校园微门户功能结构图(*号模块需实名绑定)

鉴于微信公众平台的系统约束(公众号的一级栏目最多有 3 个,二级栏目最多有五个),微门户在功能

模块设计上划分为三类:信息公开模块(又名聚焦西交)、公共信息服务模块(又名 in 交大)、综合业务服务类(又名常用查询)。二级子模块共计 13 个,如图 1 所示,其中重点信息敏感模块如微科研(项目账务,科研到账)、微财务(财务信息,学校来款,工资查询,一卡通流水)等,均需要与校内统一身份认证系统对接,完成用户实名制绑定及敏感数据加密,实现基于用户真实身份与角色的敏感信息共享服务。

4 微门户系统架构设计

如图 2 所示,西安交通大学校园微门户的整体系统架构分为四层,由底自上分别为:校园内部业务系统层、后台管理系统(微门户支撑管理系统)层、微信公众平台账号管理平台(微信公众平台)、微门户客户端层。

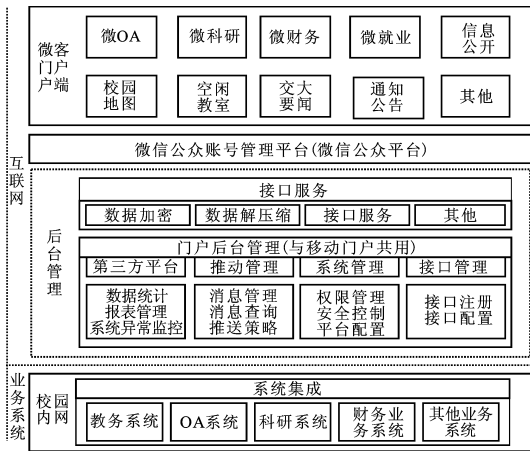


图 2 微门户系统架构图

第一层:校内业务系统层是“互联网+”校园微门户的数据基础,是为用户提供信息服务的主体数据来源(如教务系统获取教务数据、集成科研系统获取科研数据等),为用户提供掌上综合信息服务。

第二层:后台管理系统(微门户支撑管理系统)由学校自主研发,其按照功能不同分两部分建设:门户后台管理模块和接口服务管理模块:

(1)门户后台管理模块:该模块共用校园移动门户的接口管理、消息推动管理和第三方平台管理模块,接口管理模块基于下层的数据集成,为上层应用提供接口注册、接口配置服务;系统管理子模块完成基于 RBAC(Role Based Access Control)原则的用户访问权限控制与数据安全控制、平台安全配置等功能;消息推动管理模块实现客户端消息推动,消息应答及消息推送策略配置管理等;第三方平台模块完成与第三方系统监控平台(如百度统计、友盟统计等)集成,实现微门户各项运行指标的数据统计,为

系统功能优化提供重要参考。

(2)接口服务模块:该模块为数据接口提供多项数据处理与共享服务,如使用数据加解密保证数据传输阶段的安全控制、使用数据解压缩提高数据传输速率、使用接口服务为微门户上下层提供轻量级数据共享与交互功能。

第三层:微信公众账号管理平台为开发人员提供多种类衍生服务,开发人员基于 JSSDK 完成定制功能开发^[7]。

第四层:微门户客户端安装于用户智能设备中(本文直接使用微信客户端),为移动用户提供各类移动应用。页面展示采用 css+html5 的方式实现数据响应式加载和展示自适应性。基于本文系统架构实现的微门户各类微应用效果如图 3 所示(从左至右依次为信息公开、微 GIS、微科研、微财务)。



图 3 客户端各类微应用效果图

5 系统关键技术实现

5.1 消息及接口响应

5.1.1 消息自动回复

如图 4 所示,当用户通过客户端向微门户帐号发送消息时(步骤 1),微信公众账号接收该消息,根据开发人员在微信公众平台事先设定的自动回复内容进行定向自动回复。如果没有设置自动回复,管理员还可以登录微信账号管理系统对该消息进行人工回复。

5.1.2 接口交互

当用户点击微门户中的菜单项请求信息服务时,微门户公众账号接收该请求并将此请求反馈给微门户支撑管理系统(如图 4 中步骤 2B 所示);微门户支撑管理系统依据已经注册的服务接口,为用户提供服务(如图 4 步骤 3B 所示)。该过程中如果用户请求的是敏感数据,则需要进行实名制绑定,将用户的校园统一身份认证用户名与其 openid(用来标识用户微信号与微校园公众账号之间唯一对应关系的参数)进行绑定,之后微门户公众账号即可依据用户的真实身份与角色对其提供敏感数据服务(一次绑定,多次有效)。

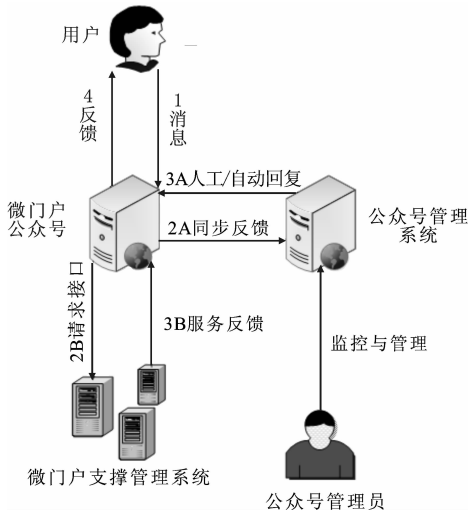


图 4 消息与接口响应模式图

5.2 实名制统一身份认证绑定

由微信公众平台开发者文档可知^[8],OpenID 是订阅某公众账号的一般用户的唯一标识符,且该 OpenID 只针对当前公众账号有效。因此获取校园普通用户与微门户公众账号之间的 OpenID 即可实现用户身份唯一标识。此外,为实现基于用户真实身份与角色,为其提供真实校园业务服务,将用户的 OpenID 与校园统一身份认证账号 NetID 进行绑定至关重要。绑定流程如图 5 所示,数据库绑定表结构如表 1 所示。

表 1 本地服务器实名绑定数据库表

字段名	含义
WeChatID	用户微信号
OpenID	用户与微门户对应编号
NetID	校内统一身份认证账号
UserNo	教工工号/学生学号
DepName	部门/学院名称
DepID	部门/学院编号
UserName	用户真实姓名
UserType	用户角色(教工/学生)

如图 5 所示,微门户支撑管理系统需在本地数据库中建立用户 OpenID 和校内统一身份认证系统(CAS)用户名的绑定关系对应表如表 1 所示,初始时空。用户使用微信客户端与微门户公众账号首次进行敏感信息交互时,微门户获取此用户的 OpenID,进行绑定。实现流程如下:

(1)当用户提出访问微门户中敏感服务时,系统判断该用户的 OpenID 是否在数据库有绑定。有绑定,则直接依据该用户的真实身份与角色为其提供

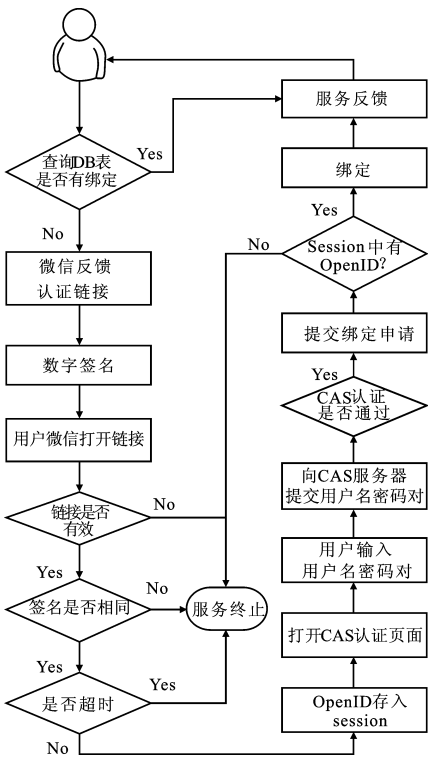


图 5 实名制认证绑定流程图

信息服务;如果没有绑定,则微信将统一身份认证链接地址反馈给用户,并进行数字签名。

(2)用户使用微信客户端打开认证链接时,判断此链接是否有效.如果链接无效则终止服务;如果链接有效,则判断数字签名是否相同(如果签名不相同则服务终止;如果签名相同,则再判断链接是否超时.如果链接超时,则服务终止)。

(3)当认证链接有效、签名匹配成功且链接未超时三个条件均满足时,微门户支撑管理系统将此用户的 OpenID 设置到用户的 session 中;然后加载校园统一身份认证页面,让用户输入其认证用户名和密码对;之后提交给校园统一身份认证服务器(CAS)进行认证。

(4)如果 CAS 认证未通过,则服务终止;如果 CAS 认证通过,则绑定申请被提交.之后微门户支撑管理系统检查 session 中是否有当前用户的 OpenID,如果没有则访问无效并拒绝服务;有 OpenID 则将此 OpenID 与 CAS 用户名进行绑定并存储到本地数据库绑定表中,之后再将该用户的 OpenID 从 session 中删除。

(5)当用户成功完成 CAS 账户(NetID)与微信账户(OpenID)绑定后,微门户即可为用户提供各类基于用户真实姓名与角色信息的敏感数据共享服务,如科研资金流转明细、财务报销及工资查询等。

最后,微门户生态系统中的每次敏感数据请求,都需要微信支撑系统检查绑定表,判断当前用户是否已经有实名制绑定.有则直接使用用户的 CAS 账号为其提供敏感服务.如果没有认证,则重复上面的绑定流程,再提供敏感服务。

5.3 RSA 加密与 MD5 签名实现

由于校园微门户为用户提供了基于用户真实身份的个性化敏感数据服务,因此针对用户真实敏感数据的保护,本文设计了 RSA 公钥加密与 MD5 摘要签名联合应用,以确保用户隐私数据不泄露,加密与签名的过程如图 6 所示。

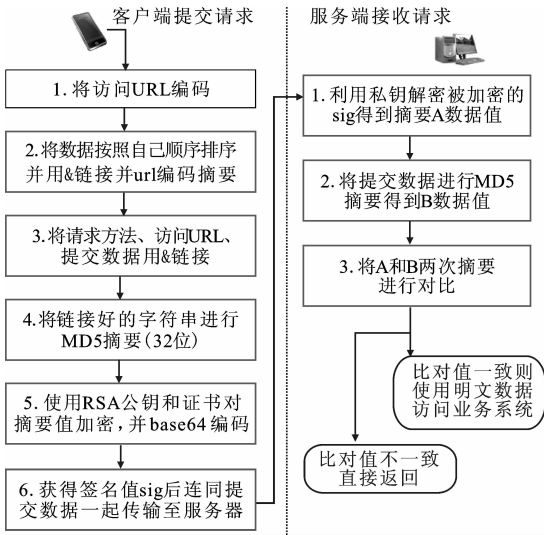


图 6 加解密工作流程图

5.3.1 客户端加密与签名实现

客户端向服务端请求敏感数据服务时,工作流程如下:

第一步:当用户通过手机微信客户端向微门户请求敏感数据服务时,微信客户端先将需要访问的 URL 进行加密编码(urlencode);之后将需要提交的数据也进行 urlencode 加密编码;然后与客户端请求的方法一起按照数据自然顺序使用“&”符号拼接成一个完成的编码串;最后对此编码串进行整体 md5 摘要计算(由步骤 1~4 所示);

第二步:客户端使用 RSA 公钥和 CA 证书(由校内统一身份认证系统提供)对上面生成的 MD5 摘要进行加密,并且把加密后生成的密文进行 base64 编码;

第三部步:基于以上工作,微门户客户端将经过 base64 编码后的密文串提交至服务端(如图 6 左侧步骤 6 所示)。

5.3.2 服务端解密与摘要匹配实现

服务端接收到来自客户端提交的访问请求后，其工作流程如下：

首先服务器使用私钥对客户端提交的密文串进行解密，计算出摘要值 A；之后，服务器将客户端提交来的数据进行 MD5 摘要获得数据值 B；接着，服务器将解密后的 A 值与 MD5 摘要后的 B 值进行比较，如果 A 与 B 相同，则使用解密后的明文与校内业务系统交互，为客户端提供服务。如果 A 值与 B 值不相同，否则拒绝服务。

6 软件测试

6.1 功能测试

软件功能测试是软件开发过程的重要环节，是查错、纠错与排错的重要过程。本文仅对部分需实名认证的重点功能(如工资查询)及消息响应机制进行测试描述。

6.1.1 敏感数据保护与实名制绑定测试

如图 7 所示，当用户(未进行过实名绑定)在校园微门户中点击“掌中财务”后，由于财务信息受加密保护与安全控制，系统拦截该用户请求；之后系统判断此用户是否经过实名认证(由于此用户未绑定，因此客户端加载西安交通大学统一身份认证页面，如图 7(b)所示)；用户输入正确的 NetID 和密码后认证通过，系统将该用户的 OpenID 与 NetID 及真实姓名等信息加入数据库中，实名制绑定成功，敏感信息成功加载(图 7(c)所示)。如果认证失败，工资页面不显示(效果图省略)。

当该用户成功完成一次实名绑定后，若其再访问其他敏感信息时，系统不再重复进行身份认证，只需从数据库中加载用户真实身份信息即可进行个性化敏感信息服务。

时响应机制。本小节以查询科研到账为例进行测试，测试过程与结果如图 8 所示。

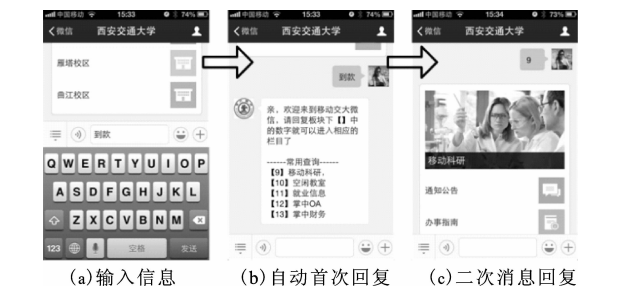


图 8 消息自动响应测试

首先用户输入消息“到账”，公共号服务器接收消息后自动回复，内容如图 8(b)所示；之后用户依据提示再输入消息编号“9”；微信公众号接收消息“9”后自动将科研到账的相关服务页面回复给用户，如图 8(c)所示；最后用户通过移动科研页面进行菜单点击，完成科研到账查询。

本案例显示基于微信公众平台进行二次开发的校园微门户可及时响应用户消息并提供综合信息共享服务。

6.2 跨平台测试

依据微信公众平台自带的软件运行跟踪统计可知，本文研发的基于 RSA 与 MD5 签名的跨平台实名校园微门户，于 2014 年上线后已经在超过 8 种移动平台上平稳运行，如表 2 所示，实现了移动微门户的跨平台需求，一次开发，多平台运行，节省大量开发与维护成本。

表 2 微门户跨平台应用支持

移动终端类型	用户数	占比/%
Android	27 170	67.33
iPhone	12 752	31.60
Wp7	350	0.87
未知	61	0.15
S60V5	8	0.02
BB10	3	0.01
S60V3	3	0.01
BB	2	0.00
S40	2	0.00

7 结束语

本文设计实现的西安交通大学微门户系统通过将微信公众平台、校园统一身份认证系统、校内各业务系统进行有机结合，实现了基于用户真实身份的



图 7 实名制绑定测试

6.1.2 消息响应测试

由于本文的研究成果是基于微信公众平台进行的二次开发，其中重要的一项功能就是移动消息及

一站式跨平台校园微门户建设,提出使用 RSA 与 MD5 联合应用的敏感数据保护机制,保障敏感数据安全;同时利用微信公众平台进行二次开发建设校园门户,极大地拓展了传统校园信息门户和校园移动门户在移动互联网领域中的覆盖率;且可在多类型智能移动操作系统运行。

本文的下一步研究计划是充分利用实名制校园微门户的客户端反馈及上下文信息,完成针对用户真实身份的大数据分析与个性化服务推荐,从而逐步实现校园微门户及核心业务的“互联网+”智慧化,为校园信息化的十三五规划做好支撑工作,更好的提升校园信息化水平。

参考文献:

[1] 童华章,吴颖骏,方伟杰,等. 学生一站式服务中心的研究与设计[J]. 中国海洋大学学报:自然科学版, 2008, 49(Sup1):33-37.

[2] 郑锋. 一站式服务架构下的电子政务应用系统[J]. 计算机工程, 2007, 33(14):249-250.

[3] Park J H, Chao H C, Chen W E, et al. Special Issue on information security and data protection in future generation communication and networking[J]. Wireless Personal Communications, 2009, 51(1):1-3.

[4] Fernandes D A B, Soares L F B, Gomes J V, et al. Security issues in cloud environments: a survey[J]. In-

ternational Journal of Information Security, 2014, 13 (2):113-170.

[5] Zhang H P, Zhang R Q, Zhao Y P, et al. Big data modeling and analysis of microblog ecosystem[J]. International Journal of Automation & Computing, 2014, 2 (2):119-127.

[6] Tsai C W, Lai C F, Chao H C, et al. Big data analytics: a survey[J]. Journal of Big Data, 2015, 2(1): 1-32.

[7] 席新亮. 微信公众平台 JSSDK 开发实战[M]. 北京:电子工业出版社,2015:1-2.

[8] 腾讯公司. 微信公众平台开发者文档[EB/OL]. [2015-12-09]. <http://mp.weixin.qq.com/wiki/11/434109e8de46b3968639217bbcb16c2f.html>.

作者简介:

洪丹丹 女,(1981-),硕士,工程师.研究方向为移动互联网技术、校园信息化关键技术.

罗军锋 男,(1976-),硕士,高级工程师.研究方向为大数据挖掘、高校信息化.

冯兴利(通讯作者) 女,(1986-),硕士,工程师.研究方向为校园信息化. E-mail:fengxingli 5927@sina.com.

徐 墨 女,(1978-),硕士.研究方向为校园信息化.

锁志海 男,(1971-),博士研究生.研究方向为数据库应用技术、高校教育信息化.

(上接第 35 页)

[3] 刘蕊洁,张金波,刘锐. 模糊 c 均值聚类算法[J]. 重庆工学院学报(自然科学),2008,22(2): 139-141.

[4] 张红旗,王春光,李海军. 基于遗传算法的草莓图像 FCM 分割方法研究[J]. 农机化研究,2015, 36(4): 55-58.

[5] 苏锦旗,张文字,薛昱. 基于改进人工免疫方法的混合模糊聚类算法[J]. 计算机系统应用,2014, 23(8): 194-197.

[6] 张慧哲,王坚. 基于初始聚类中心选取的改进 FCM 聚类算法[J]. 计算机科学,2009,36(6):206-209.

[7] 陈兴蜀,吴小松,王文贤,等. 基于特征关联度的 K-means 初始聚类中心优化算法[J]. 四川大学学报(工程科学版),2015,47(1): 16-19.

[8] 杨纶标,高英仪,凌卫新. 模糊数学原理及应用[M]. 5 版:广州:华南理工大学出版社,2011. 7.

[9] 谢娟英,高 瑞. Num-近邻方差优化的 K-medoids 聚类算法[J]. 计算机应用研究,2015,32(1):30-34.

作者简介:

贺呈磊 男,(1989-),硕士研究生.研究方向为预测与健康管理技术. E-mail:he_303560@163.com.

唐 磊 男,(1973-),研究员,硕士生导师.研究方向为空间嵌入式计算机系统结构及大容量固态存储技术.

刘 曦 男,(1979-),研究员.研究方向为卫星综合电子系统技术.