一种在 Android 移动终端实现单点登录的新方法

田 野[1],李忠献[2],崔 军[3]
(1. 中国民航大学 电子信息与自动化学院,天津 300300;
2. 北京邮电大学 计算机学院,北京 100876;
3. 天津灵创智恒软件技术有限公司,天津 300350)

摘 要:针对目前移动办公越来越普及,各大企业纷纷开发了企业内部各种各样的移动端应用系统。企业员工需要频繁登录这些应用系统,每次登录就浪费了大量时间,降低了工作效率。同时,企业员工需要记忆繁多的用户名和密码,不仅费时费力而且还存在安全隐患。因此,开发出一种能在移动端进行安全单点登录的新方法是很有必要的。通过分析移动终端上单点登录的发展前景与现状,提出了一种在 Android 设备上进行安全单点登录的新方法。该方法基于智能密码钥匙的数字证书认证技术来实现身份认证,通过 Android 应用程序显示授权资源,基于 SOAP 协议完成单点登录,实现了基于 Android 客户端的数字证书身份认证与单点登录来访问相互信任的资源。实验结果表明,该系统能支持异构系统的单点登录,用户只需一次身份认证就能访问所有授权应用,提高了用户数据安全性和工作效率,同时也为管理员的管理带来了便捷。

关键词:单点登录;数字证书;智能密码钥匙;Android 移动终端;SOAP 协议;票据
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2017)04-0145-05
doi:10.3969/j.issn.1673-629X.2017.04.032

A New Method for Single Sign-on at Android Terminal

TIAN Ye[1],LI Zhong-xian[2],CUI Jun[3]
(1. College of Electronic Information and Automation,Civil Aviation University of China,
Tianjin 300300,China;
2. College of Computing,Beijing University of Posts and Telecommunications,Beijing 100876,China;
3. Tianjin Ling Chuang Zhi Heng Software Technology Co.,Ltd.,Tianjin 300350,China)

Abstract:In view of current mobile office which is becoming more and more popular,the major companies have developed a variety of internal mobile terminal applications. Enterprise employees need to log in these applications frequently,and each time they log on to waste a lot of time,reducing the efficiency of the work. At the same time,they need to remember a wide variety of user name and password,not only time-consuming and hard work,but also the existence of security risks. Therefore,it is necessary to develop a new method which can carry on the secure single sign on the mobile terminal. Through the analysis of the prospect and present of terminal application and the existing single sign-on system,a new method for single sign-on based on Android mobile terminal is put forward. This method is based on the digital certificate technology and combines the SOAP protocol and Web Service to make the identity authentication come true. And it uses Android application instead of browser's redirection technology which can get the authorized resources. Thus the access to different application systems has been constructed by digital certificate identity authentication technology and single sign-on based on Android mobile terminal comes true. The experimental results show that this system supports single sign-on between different systems,and the user just needs to log in once to access to all the authorized resources,and that it can not only improve the efficiency of users,but also bring convenience to the administrator's management.

Key words:single sign-on;digital certificate;intelligent cipher key;Android mobile terminal;SOAP;ticket

收稿日期:2016-06-06 **修回日期**:2016-09-14 **网络出版时间**:2017-03-07
基金项目:天津市高等学校科技发展基金计划项目(20140805)
作者简介:田 野(1991-),男,硕士研究生,研究方向为信息安全;李忠献,副教授,从事网络与信息安全产品研发、工程项目管理与实施。
网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20170307.0922.068.html

1 概 述

随着移动终端和网络技术的不断发展,在商业领域,移动办公越来越受到企业的重视[1]。移动办公能给企业带来相当可观的效益,通过移动办公系统,能实现员工在任何时间、任何地点通过互联网进行工作[2],大大提高了员工的工作效率,因此各企业都在进行企业内移动办公系统的开发。对于企业内部不同办公应用的整合,比较流行的是单点登录方式。单点登录是指用户在网络中只需进行一次身份认证,即可访问所授权的所有应用,无需再次进行身份认证[3]。即“一处登录,处处登录”[4]。这样既能解决用户的安全问题和效率问题,还能给系统管理员的日常维护和管理带来方便。有很多比较成熟的商业解决方案,如 IBM 的 Tivoli Access Manager、Oracle 的 Sun Opens SO Enterprise、Netegrity Site Minder(已被 CA 收购)、Novell 的 EDirectory 等[5]。但是这些方案都是基于浏览器形式而非客户端形式,基于浏览器形式的单点登录一般无法集中管理用户的权限,而且移动终端的浏览器一般无法使用插件来完成一些必要的操作。传统的单点登录采用的身份认证方式一般都是密码口令认证,这种认证方式存在一定的安全隐患。

因此,针对上述问题,结合简单对象访问协议(Simple Object Access Protocol, SOAP)[6]与 Web 服务,提出了一种在 Android 移动终端上基于 Android 客户端应用程序(以下简称 APP)形式的安全单点登录新方法,用以解决现有 Android 移动终端信息系统中异构系统的集成、用户认证繁琐冗余、可管理性差及密码容易泄露等安全问题[7]。

用户身份认证是指通过一定的手段,完成对用户身份的确认,即确认当前所声称为某种身份的用户,确实是所声称的用户[8]。身份认证是安全的第一道大门,是各种安全措施可以发挥作用的前提。最常见的身份认证方式有账号和密码[9]。随着企业和机构引入各式各样的信息化系统,用户和管理员需要维护多个信息系统的账号和密码,影响了日常的工作效率。用户希望一次登录可以访问企业的各个信息系统,因此资源单点登录技术应运而生。

数字证书就是在互联网通信中标识通信各方身份信息的一种文件[10]。它提供了一种在网络上验证身份的方式,一般由权威的 CA 颁发[11]。数字证书存储在智能密码钥匙中,例如 USB-Key、智能 IC 卡、蓝牙 Key、指纹 Key 等设备。文中系统涉及的方法采用的是易于 Android 设备适配的蓝牙 Key。

SOAP 是交换数据的一种协议规范,是一种轻量级的、简单的、基于 XML 的协议,它被设计成在 Web 上交换结构化和固化的信息[12]。此次采用 SOAP 协议来完成单点登录过程中的票据兑换。

目前常见的单点登录模型包括以服务器为中心的单点登录、以客户端为中心的单点登录和客户/服务器模式的单点登录。下面分别介绍它们的优缺点。

以服务器为中心的单点登录解决方案:所有的认证信息都存储在中心服务器的数据库上,当需要对用户进行身份认证时,这个中心服务器与系统内其他所有设备进行通信。这种通信需要中心服务器与应用服务器集成,即在单点登录服务器上开发应用系统的客户代理。该方案的优点是有单一的控制点,方便对资源的访问进行控制和权限管理[13]。缺点是与外部应用支持比较困难,容易出现冗余,需要考虑负载均衡和备份。这种模型的代表就是微软的 Passport 单点登录技术。

以客户端为中心的单点登录解决方案:所有的认证信息存储在用户的客户端,需要在客户端部署专门的单点登录代理。优点是不需要在后端集成,单点登录服务器能支持大部分应用,由于认证信息存放在客户端,可以在任何时间访问业务。缺点是由于使用密码代填的方式,若数据传输过程中没有加密,则账号密码容易泄露,而且没有控制点,无法实现细致的权限控制。

客户端/服务器模式的单点登录解决方案:该方案是以上两种方案的结合,具有单一的访问控制点并且由客户端的代理提供认证。在服务器一侧有两种实现方法,一种是独立网关式,即在服务器前部署单点登录代理;另一种是嵌入式方式,即将服务器端的单点登录代理的功能以单点登录 API 的形式集中在应用服务器中。这种方案具有两者的优点,具有单一的访问控制点,便于实现集中、细致的权限控制。这种模型的代表就是 Kerberos[14]。

所介绍的单点登录解决方案,就是基于客户端/服务器模式的。该方案在移动终端上实现的难点在于如何设计针对 Android 移动客户端的 Web 服务以及如何在 SOAP 中传输票据信息(tickets)。该方案基于单独的认证服务器和单点登录服务器进行身份认证和票据的获取与兑换,利用 SOAP 协议进行异构系统间票据信息的传递,很好地实现了在 Android 移动端上认证一次后即可访问所有授权应用的功能。

2 系统架构与设计

2.1 系统框架

该系统实现的是基于 APP 形式的单点登录新方法,同时结合了数字证书身份认证技术。该方法的实现需要如下组成部分:智能终端(Android 设备)、智能卡密码钥匙(蓝牙 Key)、APP、身份认证服务器、单点

登录服务器、资源服务器。系统基于以上模块,结合 SOAP 协议和 Web 服务,在保证系统安全的情况下,更好地实现了移动端的单点登录操作。其系统框图如图 1 所示。

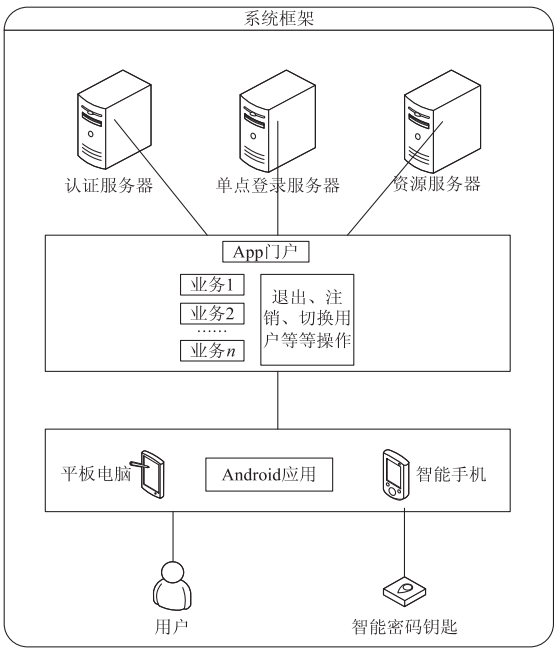

图 1　系统框架

智能终端:主要指 Android 设备,包括 Android 智能手机和平板电脑。用户通过智能终端上的 APP,进行身份认证以及相关的业务操作,操作结果通过智能终端显示给用户。

智能卡密码钥匙:指存放数字证书的设备,在该系统指蓝牙 Key。用户每次在打开 APP 之后,进行身份认证时会连接 Key,读取 Key 中的数字证书信息,并对数据进行签名验签等操作。

APP:是指在智能设备上实现身份认证、展示授权资源和单点登录等功能的一个客户端应用程序。用户通过该程序对业务进行操作,也是通过该程序实现了身份认证、单点登录等操作。

身份认证服务器:即部署身份认证服务的服务器。在用户打开 APP 进行身份认证时,智能终端通过连接蓝牙 Key,使用获取到的公钥证书表明身份和对应的私钥签名证实身份,进而实现在智能终端上对用户的身份进行认证。

单点登录服务器:即部署单点登录服务的服务器。对通过身份认证的用户进行相应资源的单点登录,使其获取到访问授权资源的票据,最终能实现对授权资源的单点登录。

资源服务器:即部署资源的服务器。包括用户办公使用的业务系统和资源,例如邮件系统,人事管理、财务管理等应用。

该系统的典型应用场景:企业中的用户通过平板电脑或者手机,登录 APP,使用自己独有的智能密码钥匙进行认证,登录之后可以查看他所拥有访问权限的资源,比如工资系统、企业 OA 系统、邮件系统等,其他用户也只能看到自己拥有访问权限的资源。

2.2　移动终端单点登录业务的流程

移动终端基于数字证书的单点登录流程如图 2 所示。

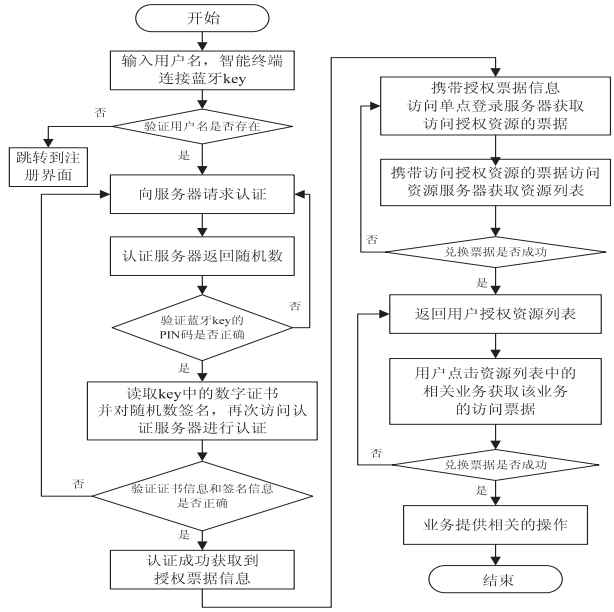

图 2　流程图

客户端获取授权资源列表的详细流程如下:用户打开 APP,输入用户名,连接蓝牙 Key,访问认证服务器请求认证;认证服务器检查用户名并响应认证请求,返回一个随机数,蓝牙 Key 对该随机数进行签名,用户需输入蓝牙 Key 的 PIN 码,若连续五次输入 PIN 码错误,Key 会自动锁定。蓝牙 Key 执行签名操作后,APP 会把该签名值发送到认证服务器进行认证;认证服务器收到认证信息后,进行公钥验签操作,若验证正确,则返回一个认证成功的标识(token),APP 凭借此标识向单点登录服务器获取用户对资源的授权信息票据(tickets),若验证失败,则返回认证界面重新请求认证。APP 携带用户对资源的 tickets 去访问资源服务器,资源服务器与单点登录服务器进行票据的兑换,兑换成功后单点登录服务器返回该用户的用户名(username),资源服务器则在数据库表中查出该用户的授权资源列表,并返回 APP 呈现给用户;若票据兑换失败,则重新请求用户对资源的 tickets。

经过以上步骤,用户获得其授权资源,之后单点登录访问不同应用的流程如下:用户点击相应的应用,APP 向单点登录服务器申请该应用的 tickets,单点登录服务器根据 username 返回票据。客户端携带该票据去访问业务,该业务访问单点登录服务器兑换票据并验证,验证成功则显示业务。当用户对某一应用操

作完成后,退出该应用;当需要访问其他应用时,在资源列表界面重复上面的步骤即可访问其他应用。

用户操作完应用后,退出 APP,此时客户端会清除所有的 tickets 信息和用户信息。再次打开客户端时,需重新进行以上的所有操作来进行单点登录访问应用。

3 关键问题的实现

系统采用基于 ESB 模型的服务,WebLogic 应用服务器,LDAP 服务器以及 Eclipse(ADT)开发平台实现了基于移动端的数字证书单点登录;采用 XML 协议实现对 Webservice 的发布、查找、绑定与描述;采用 SOAP 协议来进行移动端与服务器之间的票据信息的传递。

3.1 Web 服务的设计

Webservice 是连接服务器与移动端的桥梁。移动端通过访问 Webservice 来传递认证服务器所需的数据;认证服务器通过 Webservice 返回给移动端相应的结果。单点登录服务器也通过 Webservice 以及 SOAP 消息向移动端传递和兑换票据信息。有关 Webservice 的描述语言如下:

```
认证请求的 Webservice:
<xs:elementname = " authenticationByCertificate" type = " tns:
authenticationByCertificate"/>
<xs:complexTypename = " authenticationByCertificate" >
<xs:sequence>
<xs:elementname = " credentials" type = " tns:userCertificateCre-
dentials" minOccurs = "0"/>
<xs:element name = " serviceUrl" type = " xs:string" minOccurs
= "0"/>
</xs:sequence>
</xs:complexType>
<xs:complexTypename = " userCertificateCredentials" >
<xs:sequence>
<xs:elementname = " certificate" type = " xs:base64Binary" mi-
nOccurs = "0"/>
</xs:sequence>
</xs:complexType>
```

在 Webservice 的描述中,该 Service 的名称为 authenticationByCertificate,进行认证需要移动端传入的参数为 credentials 和 serviceUrl,其中 credentials 是由 base64 编码的签名信息,serviceUrl 是字符串类型的服务器地址。

3.2 SOAP 消息

SOAP 协议为不同的系统间交换数据提供了一个很好的途径。在整个流程中,基于 SOAP 的票据申请与兑换共进行了两次,一次是对授权资源的票据的申请与兑换,另一次是访问授权业务的票据的申请与兑换。每次票据的申请与兑换经过如下的几个过程:APP 构造 SOAP 请求、服务器接收并解析 SOAP 请求、服务器生成返回的 SOAP 消息、APP 接收并解析收到的 SOAP 消息。以访问授权业务票据为例,其申请与兑换的 SOAP 消息的具体代码设计如下:

在获取到授权资源列表后,用户通过点击相关应用,访问单点登录服务器票据申请接口去申请票据,其数据格式设计为:

```
<soapenv:Envelope xmlns:soapenv = " http://schemas. xml-
soap. org/soap/envelope/" xmlns:tic = "http: //ticket. com" >
<soapenv:Header/>
<soapenv:Body>
<tic:CreateTicket>
<username>Administrator</username>
</tic:CreateTicket>
</soapenv:Body>
</soapenv:Envelope>
```

返回的信息为经过 base64 编码的票据信息。其格式设计为:

```
< ns2: CreateTicketResponse xmlns: ns2 = " http://ticket.
com" >
<return>CHSJAJYEEDSSASSDKJFLD = = </return>
</ns2:CreateTicketResponse>
```

此时 APP 携带收到的票据去访问相应资源,资源收到票据后,会访问单点登录服务器兑换票据接口来兑换用户信息,其格式设计为:

```
<tic:obtainUserByTicket>
<ticket>CHSJAJYEEDSSASSDKJFLD = = </ticket>
</tic:obtainUserByTicket>
```

单点登录服务器返回票据兑换的结果为经过 base64 编码的用户名。其格式设计为:

```
<ns2:obtainUserByTicketResponse xmlns:ns2 = " http://ticket.
com" >
<return>Y2hlbmppZQ = = </return>
</ns2:obtainUserByTicketResponse>
```

4 系统测试与结果分析

该系统使用了身份认证服务器和单点登录服务器,相关的应用部署在不同服务器上。测试时所使用的移动终端包括不同 Android 系统版本的 Android 手机/平板电脑平台以及电脑端的单点登录平台;测试中所使用的 Key 包括海泰方圆公司和飞天诚信公司的两款常用的蓝牙 Key。不同 Android 系统版本和不同品牌 Key 对该应用的适用和支持情况如表 1 所示。

测试结果表明,在不同的 Android 系统版本和不同品牌的蓝牙 Key 的环境下,通过一次蓝牙 Key 的身份认证后,客户端均能成功获取到授权资源列表,再次点击相应的应用后,均能成功访问应用。说明在不同

的 Android 移动终端上,系统的适用性很强,能够很好地实现单点登录访问资源的功能。

表 1　不同 Android 系统及不同 Key 对应用的适用情况表

Android 版本是否支持该应用	海泰方圆多功能—蓝牙液晶 Key	飞天诚信二代音频/蓝牙 Key
Google 原生 Android 4.4	支持	支持
Google 原生 Android 5.0	支持	支持
小米 MIUI6	支持	支持
魅族 Flyme4.5	支持	支持

为了测试该系统相比于传统的电脑端基于浏览器重定向形式的单点登录所具有的优势,对二者单点登录访问资源所花费的时间进行对比。测试中,蓝牙 Key 选用海泰方圆公司蓝牙 Key 作为移动终端单点登录的典型,让同一用户在两种平台下去访问同一资源,计算登录时间和访问资源的响应时间。测试结果如表 2 所示。

表 2　不同平台单点登录的响应时间

Key 型号	Android 手机魅族 Flyme4.5 系统	电脑端浏览器形式
海泰方圆多功能—蓝牙液晶 Key	登录系统用时小于 1 s,登录资源用时小于 1 s,用户感觉基本没有停顿时间	登录系统用时 3 ~ 5 s,登录资源用时 2 ~ 3 s,用户能明显感觉等待时间

测试结果表明:通过在移动终端上采用基于 Android 客户端形式的单点登录,结合 SOAP 协议与 Web 服务,同时使用数字证书密码钥匙,更好地保证了身份认证的安全性与快捷性。相比原有的分散的应用认证方式以及传统的基于浏览器重定向的单点登录方式,减少了系统响应时间,系统效率和可用性也大大增加。同时,基于 Android 客户端形式的单点登录适用于不同版本的 Android 平台,也能很好地兼容不同厂商的蓝牙 Key,更好地保证了该方法的实用性。

5　结束语

在企业移动办公越来越流行的今天,移动端的单点登录的作用显得尤为突出。在移动终端上实现的基于 Android 应用的单点登录新方法,采用 SOAP 协议与 Web 服务相结合,将操作系统不同、编程语言不同、数据库不同的应用系统与认证服务器和单点登录服务器进行整合,解决了异构系统间互操作的问题,提高了认证的效率与灵活性,也为用户信息的管理带来了方便。同时,使用蓝牙 Key 和数字证书技术,完美地保证了系统的安全性;而且使用 Android 应用程序形式,在移动终端较小的屏幕上将应用更好地展现给用户,大大提高了系统的便捷性和用户的可操作性。相比传统的单点登录形式,效率有了很大提高,该方法为移动端的单点登录方法提供了一个新思路。

参考文献:

[1] 孟青春,吴颖川,刘志勤,等. 基于移动终端的多终端单点登录研究与设计[J]. 计算机工程与设计,2014,35(5):1536-1541.

[2] 王小红. 基于 Cookie 的单点登录认证机制实现[J]. 重庆工商大学学报:自然科学版,2014,31(8):73-78.

[3] Chen Yebin, Xia Bing, Wu Baozhu, et al. Design of web service single sign-on based on ticket and assertion[C]//2nd international conference on artificial intelligence, management science and electronic commerce. [s. l.]:[s. n.],2011.

[4] Ye Q, Bai G, Wang K, et al. Formal analysis of a single sign-on protocol implementation for Android[C]//20th international conference on engineering of complex computer systems. [s. l.]:[s. n.],2015.

[5] Yulin T, Feng Z. The analysis and design for single sign-on in the mobile application data center[C]//3rd international conference on system science, engineering design and manufacturing informatization. [s. l.]:[s. n.],2012.

[6] Armando A, Carbone R, Compagna L, et al. An authentication flaw in browser-based single sign-on protocols: impact and remediations[J]. Computers & Security, 2013, 33(4): 41-58.

[7] 陈萱华,林淑玲,杨　玲. 云环境下跨域单点登录解决方案[J]. 现代电子技术,2015,38(2):49-51.

[8] 王冠众,张　斌,费晓飞,等. 基于可转换代理签密的 SAML 跨域单点登录认证协议[J]. 计算机科学,2015,42(4):106-110.

[9] 李晓永,王福喜. 基于票据的单点登录系统设计与实现[J]. 现代电子技术,2015,38(13):85-89.

[10] 邹晓辉. 一种基于数字证书的跨域单点登录解决方案[J]. 长春工业大学学报:自然科学版,2010,31(6):683-686.

[11] 朱　青. 基于 CAS 的单点登录系统的设计与实现[D]. 北京:北京工业大学,2014.

[12] 霍成义. 结合 Cookie 与票据共享的单点登录方案[J]. 自动化与仪器仪表,2013(3):161-163.

[13] 吴晶晶. PKI 关键理论与应用技术研究[D]. 合肥:中国科学技术大学,2008.

[14] 宋小龙. 基于数字证书认证的单点登录系统设计与实现[D]. 大连:大连理工大学,2014