

# 基于 PKI 的校园移动应用身份认证设计

沈斌表<sup>1</sup>, 毛海波<sup>2</sup>, 刘柏嵩<sup>2</sup>

(1. 宁波大学 后勤管理服务处, 浙江 宁波 315211; 2. 宁波大学 图书馆与信息中心, 浙江 宁波 315211)

**摘要:** 运用公开密钥基础设施非对称密码算法原理和技术, 设计了基于 PKI 的移动应用身份认证系统. 详细阐述了该身份认证系统的模块结构、模块功能以及数字证书的验证流程, 可为相关应用提供参考.

**关键词:** PKI; 移动应用; 身份认证

**中图分类号:** TP393

**文献标志码:** A

**文章编号:** 1001-5132 (2014) 02-0055-04

随着校园 WiFi 无线网络的建成, 校园移动应用系统得到快速的建设和使用, 使校园信息化服务在时间、空间上得到延伸, 可让任何人在任何时间、任何地点、任何移动终端设备来享受校园移动服务. 当前, 移动应用系统的身份认证一般采用用户名加口令的身份认证机制, 采用这种认证模式的移动应用系统在身份认证、数据完整性和数据机密性等方面存在一定的安全问题. 如何让移动用户的内容访问和信息安全得到保障是移动应用系统建设所要解决的最重要、最基本的问题, 笔者将结合 PKI 身份认证技术, 采用 X.509 数字证书的强身份认证模式<sup>[1]</sup>, 对用户的身份认证、访问控制、安全审计以及保护用户信息安全等方面进行探讨.

## 1 身份认证技术

身份认证是在计算机网络中确认操作者身份的过程<sup>[2]</sup>, 身份认证技术则是在计算机网络中确认操作者身份的过程而产生的有效解决方法. 根据移动应用系统安全保护要求, 人们提出了不同类型的身份认证技术, 其中有口令认证、令牌认证、基于 PKI 的数字证书认证<sup>[3]</sup>以及基于指纹、虹膜、面容等人体生理特征的“生物认证”等.

### 1.1 认证模式

单向身份认证是指信息从用户 A 到用户 B 的单向传送, 即  $A \rightarrow B: \{T_A, R_A, B\}[T_A, R_A, A]$ , 其中,

$\rightarrow$  表示信息发送,  $\{ \}$  表示需发送的信息,  $[ ]$  表示接受信息所需做的计算,  $T_A$  表示 A 发出的时间戳,  $R_A$  表示 A 发送信息时产生的随机数.

双向身份认证是指信息从用户 A 到用户 B, 再从用户 B 到用户 A 的双向传送, 即  $A \rightarrow B \rightarrow A: \{T_A, R_A, B\}[T_A, R_A, A]\{T_B, R_B, A\}[T_B, R_B, B]$ , 其中,  $T_B$  表示 B 发出的时间戳,  $R_B$  表示 B 发送信息时产生的随机数.

可信任第三方的认证是指用户 A 要访问系统 B, 首先信息从用户 A 向可信第三方 C 申请访问系统 B, 在可信第三方 C 确认用户 A 有权访问系统 B 后, 那么用户 A 和系统 B 才建立通信信道, 则用户 A 可以访问系统 B.

分布式认证是指信息从用户 A 向网络中的多个认证系统发出认证请求<sup>[4]</sup>. 分布式认证将整合多个认证系统的判决结果来进行网络身份认证, 这种认证模式可降低单模式认证的脆弱性.

### 1.2 几种常见的身份认证技术

目前, 用户身份认证主要技术有口令认证、基于生物特征的身份认证、双因素身份认证技术、Kerberos 认证技术以及基于 PKI 的身份认证等.

口令认证技术是最常用的一种认证技术, 它分为可重用口令认证技术和动态口令认证技术. 其中, 可重用口令认证是最常用、最简单的认证技术, 且口令是一组固定的代码; 而动态口令认证是

通过加密终端设备随机产生、不断变化、没有重复的一种口令。

生物特征认证技术是以人体可靠的、唯一的以及稳定的生物特征为基础,并结合计算机的图像处理 and 识别技术来验证用户身份的技术。目前,常见的有指纹识别、脸部识别、虹膜识别、掌纹识别等技术。

双因素身份认证技术是指一个因子在使用时才知道密码<sup>[5]</sup>,另一个因子在加密终端设备生成动态口令,两者均正确时才能确认用户身份。如 ATM 机上使用银行卡必须具备两个条件——银行卡(硬件部分)和密码(软件部分)。

Kerberos 认证技术是基于对称密码体系的可信第三方认证鉴别协议<sup>[6]</sup>。Kerberos 是应用在分布式的 Client/Server 体系结构中,采用一个或多个 Kerberos 服务器提供鉴别服务。

## 2 PKI 身份认证技术

### 2.1 PKI 的体系结构及其功能

公开密钥基础设施(Public Key Infrastructure, PKI)是用非对称密码算法原理和技术实现并提供安全服务的具有通用性的安全基础设施<sup>[7-8]</sup>。PKI 的策略、软硬件系统(认证服务器、目录服务器、PKI 系统等)、认证中心(Certification Authority, CA)、注册机构(Registration Authority, RA)、证书发布系统、PKI 应用以及 PKI 应用接口系统(API)等构成了一个完整的 PKI 认证体系(图 1)。

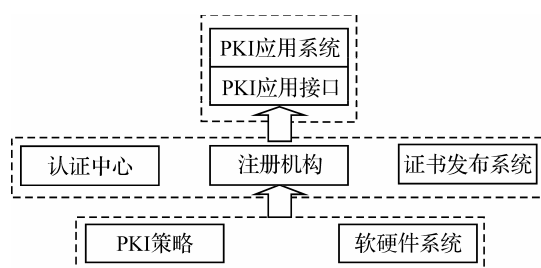


图 1 PKI 的体系结构

一个典型、完整、有效的 PKI 系统应该具备证书生成、证书注销、存储和检索证书与 CRL、提供信任、证书链处理、交叉认证、时间戳、密钥生成、密钥注销、密钥恢复、密钥更新、密钥归档、密钥备份等功能。PKI 系统为不同用户按不同需求提供认证服务、数据完整性服务、数据保密性服务、

不可否认性服务、公正服务及时间戳等服务。

### 2.2 用户身份认证流程

基于 X509 的数字证书是 PKI 认证用户的唯一标识,它由认证中心统一管理和颁发。

要获得基于 X509 的数字证书需要完成以下三个步骤:首先,用户向注册机构提供个人信息,注册机构对个人信息进行审核,同时提交到认证中心。如果用户符合认证中心的安全策略,那么就为用户颁发一份认证中心内具有唯一标识的用户证书。其次,认证中心根据用户证书向密钥管理设备申请用户证书的 RSA 公私密钥数据<sup>[9]</sup>,成功后将公私密钥数据返回给认证中心,同时在密钥管理设备中备份这对 RSA 公私密钥数据。最后,认证中心将公私密钥数据封装成数字证书格式,并保存到用户的 USB 等数字证书载体中。

用户在认证中心所信任的系统中身份认证过程如下:首先,用户接入系统时,服务端获取用户数字证书数据,判断该证书是否属于本中心的数字证书。其次,如属于本中心,服务端使用 LDAP 目录服务协议或 OCSP 在线状态查询协议向认证中心确认证书是否过期、撤销等信息。最后,服务端与客户端双方均确认双方是在同一个认证中心体系下,并且判断数字证书有效,那么用户身份认证成功。

## 3 基于 PKI 技术的移动应用身份认证设计

### 3.1 移动应用身份认证的模块设计

移动应用身份认证过程将涉及到用户移动终端设备、无线网络、身份认证系统和无线应用系统,移动应用身份认证框架结构如图 2 所示。

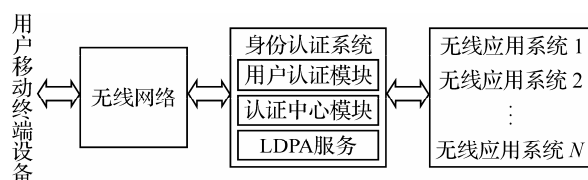


图 2 移动应用身份认证框架

其中,身份认证系统是移动应用身份认证过程的核心部分,它是由认证中心模块、用户认证模块和 LDAP 目录服务三部分组成。

(1) 用户认证模块负责实现用户与移动应用之间的安全连接和身份认证。双方都通过数字证

书确认身份,而身份确认通信采用SSL协议以确保认证的安全性。身份认证主要是对证书的路径、签名、有效期以及是否撤销等进行验证,而且每个验证都需同时通过,才能说明证书是有效的。

(2) 认证中心模块为数字证书提供申请、审批、颁发、查询、备份、更新、验证和撤销功能,是身份认证系统的基础模块。

(3) LDAP 负责保存数字证书,它是一个公共信息库。同时,还负责获取用户的公钥,并验证用户身份的合法性。

### 3.2 移动应用身份认证模块的功能设计

移动应用身份认证模块采用LDAP和用户间双向的高强度身份认证模式,其前提是双方必须拥有可用于密钥交换的数字证书。用户和LDAP实现双向认证的过程分为三步:

首先,用户向LDAP发送认证请求信息,LDAP在收到信息后向用户发送LDAP的数字证书,用户收到LDAP数字证书后,马上进行验证。如果验证不成功,通信中断;如果验证成功,则向LDAP发送用户数字证书。当LDAP收到证书后,马上进行验证。如果验证不成功,通信中断;如果验证成功,向用户发送成功消息。

其次,用户端自动生成一个随机数,并通过对称密钥算法计算获得会话密钥。用户从LDAP证书中获取公钥,并用公钥对此随机数进行加密,再将加密数据发送给LDAP。当LDAP收到加密数据后,就用自己的私钥进行解密,进而得到此随机数,最后再用同样的对称密钥算法计算出与用户端同样的会话密钥。

最后,LDAP使用用户的公钥对随机数进行加密,再回传给用户端。用户端收到加密数据后,用自己的密钥解密,最后比较两个随机数是否一致,如果一致则向LDAP发出确认消息,确定安全信道已经建立,完成这次认证过程。

### 3.3 证书验证模块的功能设计

数字证书的验证过程包括验证数字证书路径、数字证书签名、数字证书有效期和数字证书是否被撤销四个步骤,只有验证全部通过才能确定数字证书有效。

(1) 验证数字证书路径。数字证书路径要具备一个典型的树形结构,本级数字证书为叶节点,验

证过程则是叶节点向父节点逐级向上验证,直到根节点。满足这种叶节点→父节点→根节点的证书关系链才是完整的路径,如果某级不能满足,则数字证书无效。

(2) 验证数字证书签名。用父节点的数字证书公钥对子节点数字证书中的签名部分进行RSA加密计算,得出1个摘要信息A。再用哈希算法对子节点数字证书中未签名部分进行RSA加密计算,得出1个摘要信息B。最后,比较A值和B值,如果相等,则数字证书签名有效,反之,则数字证书无效。验证过程就是根节点向子节点逐级向下验证,直到叶节点数字证书。

(3) 验证证书有效期。数字证书都有个有效期限,且只有在有效期内才能正常使用。验证的方法是先取出数字证书中的有效日期,再与本地当前日期进行比较,最后,判断数字证书是否在有效期内。验证过程就是根节点向子节点逐级向下验证,直到叶节点数字证书,确保数字证书路径上的证书都有效。

(4) 有限期内的数字证书还需验证是否被撤销。验证方法是到证书撤销列表CRL中检查数字证书是否在其中,判定数字证书是否已被撤销。

### 3.4 用户数字证书验证流程设计

移动应用身份认证的实质就是用户数字证书的验证过程。用户数字证书的验证既要验证本级数字证书,还要验证数字证书链上每张数字证书的有效性。其验证流程主要由以下步骤组成:

(1) 用户通过移动终端设备,经无线网络访问移动应用程序,身份认证系统要求用户出示数字证书,并获取用户数字证书。

(2) 从用户数字证书公钥证书文件中取出待验证的数字证书主体信息、签名算法标识和签名值。

(3) 分析并提取数字证书主体信息中的数字证书序列号和有效期。

(4) 从当前最新的数字证书撤销列表中获取撤销数字证书链信息。

(5) 在撤销数字证书链中检查是否有步骤(3)中的数字证书序列号,如没有序列号则标注该数字证书未被撤销,反之,验证无效。

(6) 从步骤(3)中取出数字证书有效期( $D_1$ ),再从本地取出当前日期( $D_2$ ), $D_2 \geq D_1$ 数字证书有效,

$D_2 < D_1$  验证无效.

(7) 从父节点数字证书中取出公钥信息( $M$ ).

(8) 用  $M$  对步骤(1)中的数字证书签名值进行解密, 得出哈希值( $H_1$ ).

(9) 根据步骤(1)中的签名算法标识(哈希算法)对未签名的数字证书主体信息进行哈希计算, 得出哈希值( $H_2$ ).

(10) 比较  $H_1$  和  $H_2$  哈希值, 如果  $H_1 = H_2$ , 则数字签名验证成功, 反之, 验证无效.

只有当步骤(4)、(6)、(10)都验证通过, 才判定数字证书有效, 否则, 数字证书无效.

### 3.5 移动应用系统身份认证实现

移动应用身份认证系统采用基于 J2EE 软件框架结构, 运行在 SDK1.5 环境中, 系统是用当前最流行的 JAVA 开发软件——Myeclipse 10 开发工具开发. 按照移动应用身份认证系统的设计要求, 逐步实现移动应用身份认证系统的用户与服务器端的双向认证、数字证书的申请、审批、颁发、查询、备份、更新、验证和撤销功能等功能模块. 本移动应用身份认证系统具有良好的安全性、开放性、可靠性、可扩展性和可移植性, 支持分布式计算, 具有跨平台型, 还能支持多种移动终端.

## 4 结语

身份认证系统可以在用户的身份认证、访问控制、安全审计以及保护用户信息安全等方面得到有

效地保护, 采用 PKI 身份认证技术的身份认证系统, 能够更好的解决移动应用系统中普遍遇到的数据机密性、安全性及完整性等关键问题, 做到身份认证准确和高效, 访问控制有效和安全, 能够更好的保护用户的隐私信息.

### 参考文献:

- [1] 袁晖. 基于 X.509 证书的身份认证机制的研究[J]. 大众科技, 2006(2):174-175.
- [2] 刘忆成. 电子身份认证中生物辨识技术法律问题比较研究[J]. 信息网络安全, 2011(3):31-33.
- [3] 关振胜. 公钥基础设施 PKI 及其应用[M]. 北京: 电子工业出版社, 2008:1-417.
- [4] 刘柏嵩, 毛海波, 沈斌表. 基于 Shibboleth 的校际跨域认证研究与实现[J]. 宁波大学学报: 理工版, 2012, 25(2):33-36.
- [5] 周国良. 双因素身份认证技术研究[J]. 技术论坛, 2003(10):37-38, 41.
- [6] 秦小龙, 杨义先. USB 密码钥及其在 Kerberos 系统中的应用[J]. 计算机工程与应用, 2002(5):12-14.
- [7] 汤彬, 胡浩民. 基于 PKI 身份认证技术的研究与实现[J]. 自动化仪表, 2008, 29(9):16-21.
- [8] 解晓东. 基于数字证书的身份认证技术研究[D]. 青岛: 中国海洋大学, 2009.
- [9] RSA. Secure ID authentication: A better value for better ROL[EB/OL]. [2003-12-01]. <http://www.rsasecurity.com/pructs/secrid/whitepaper/bvbr0iwp1201.pdf>.

## Design for Campus Mobile Application Identity Authentication Based on PKI

SHEN Bin-biao<sup>1</sup>, MAO Hai-bo<sup>2</sup>, LIU Bai-song<sup>2</sup>

( 1.Logistics Department, Ningbo University, Ningbo 315211, China;

2.Library & Information Center, Ningbo University, Ningbo 315211, China )

**Abstract:** In this paper, the public key infrastructure (PKI) asymmetric cryptographic algorithm is designed for mobile applications based PKI authentication system. Also, the authentication system's the module structure, the module features and digital certificate verification process are reviewed in detail, and can provide a reference for the relevant application.

**Key words:** PKI; mobile applications; identity authentication

(责任编辑 章践立)