基于 B/S 和 C/S 混合模式的 CA 证书发放实现*

黄　锐, 李　涛, 王姝妲, 王志明, 丁勇雷, 刘颖娜
(四川大学 计算机学院, 四川 成都 610065)

摘　要: 提出了一种基于 B/S 与 C/S 混合模式的 CA 证书发放系统, 该系统的实现采用多层体系架构, 将应用独立的认证中心与应用相关的权限访问控制成功地相结合, 实现了证书与用户权限的绑定, 并成功地运用于电子政府的具体应用中。

关键词: 公钥基础设施; 认证中心; Zend
中图法分类号: TP393.08　　**文献标识码:** A　　**文章编号:** 1001-3695(2006)03-0113-03

Implement Certificates Distribution of CA Based on B/S and C/S Mode

HUANG Rui, LI Tao, WANG Shu-Da, WANG Zhi-ming, DING Yong-lei, LIU Ying-na
(Dept. of Computer Science, Sichuan University, Chengdu Sichuan 610065, China)

Abstract: This paper presents a kind of compounded certificates distribution system based on B/S and C/S mode, the implementation of this system adopts a multi-tier architecture, and successfully conbines the application independent Certificate Authority and the application dependent priviledge access control, finally, completes the binding between certificate and the priviledge. This system is successfully applied in the Electronic Government affairs.

Key words: PKI; CA; Zend

公钥基础设施(Public Key Infrastructure, PKI)[1]在标准的制定和实现技术上日趋完善。出于网络安全方面的考虑, 越来越多的电子商务、电子政务平台选择 PKI 作为应用系统开发的基础。然而在实际应用中, PKI 只是提供了对于身份认证、数据加密、获得证书等较好的支持, 并没有在访问权限的控制上提供较好的解决方案[2]。在具体开发过程中, 所面临的问题是: 作为 PKI 的核心部分——认证中心(Certificate Authority, CA)如何结合访问权限控制, 从而安全有效地应用在现今的电子商务、电子政务平台中。

由四川大学计算机网络与安全研究所独立研发的“四川省政府采购平台”作为四川省一项电子政务的实施, 成功地运用了基于 B/S 与 C/S 混合模式的多层次体系架构, 实现了 PKI 应用框架与权限访问控制相结合, 最终提供了网上安全招标、投标等政府职能服务。源于该平台的开发, 本文给出了在 PKI 与权限控制相结合的情况下, 如何采用该混合模式下的多层次体系架构实现认证中心的证书发放功能。

1　相关技术

目前, 在多层体系结构的应用中, 主要由客户端、中间件和后台数据库三部分组成。应用服务程序构建在中间件和后台数据库之上, 而应用客户程序则构建在客户端和中间件之上, 中间件负责客户程序与服务程序之间的通信。在本系统的实现中, 中间件采用 CORBA, 而 Web 服务器中采用 PHP 的核心 Zend 的扩展技术。

1.1　PHP 的核心 Zend

作为开源项目的 PHP, 在 Web 应用的开发中得到了广泛使用, 通常被用作开发客户端程序。Zend[3]作为 PHP 执行的引擎, 承担了 PHP 语言的分析、翻译、执行的功能。Zend 实现了 PHP 中的标准数据结构, 而且还提供了与外部资源和协议的访问接口。利用扩展功能模块接口, 程序员就可以编写自己的功能模块(类似 MySQL 那些模块), 直接通过 PHP 脚本语言来访问特定的外部资源。模块以动态加载的形式被调用, 所以只编译模块即可, 没有必要编译整个 PHP。

为了编写扩展的功能模块, Zend 提供了完整的 C 语言函数库和宏, 如 emalloc(), 类似 C 语言中的 malloc()。下面是编写一个功能模块必要的步骤: ①包含头文件“php.h”, 该文件包含 Zend 提供的宏定义及函数定义; ②声明导出函数, 导出函数就是可以在 PHP 语句中调用的, 但其实现是放在编写的功能模块中; ③将导出函数加入模块定义中; ④用 C 编译器直接编译, 并在 PHP 的配置文件中加入模块的名字。以后在编写 PHP 程序时, 调用自己的导出函数就与调用 PHP 自带的函数一样。

2　认证中心证书发放实现

2.1　系统结构

整个系统主要分为两部分, 如图 1 所示。虚线内表示与应用无关的部分, 主要是认证中心的实现部分, 用于生成证书; 虚线外表示了具体应用, 这里演示的就是政府采购平台中的权限

收稿日期: 2005-03-03; 修返日期: 2005-04-25
基金项目: 国家自然科学基金资助项目(60373110); 教育部博士点基金资助项目(20030610003)

管理部分的实现。可以从图 1 中清楚地看出,虚线内采用的是 C/S 模式,而虚线外采用的是 B/S 模式。

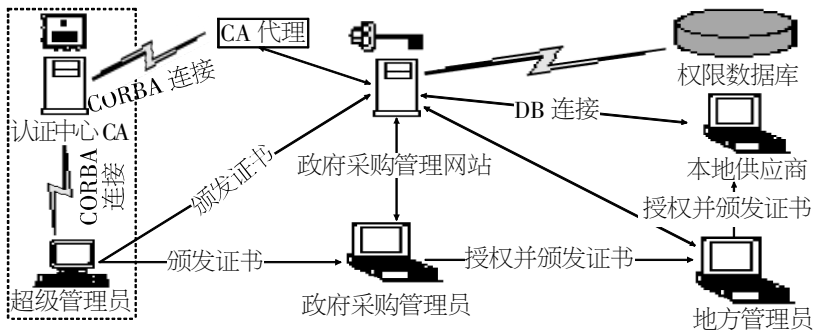

图 1 系统结构

2.2 具体应用流程

由于该平台是安全的电子政务平台,所以图 1 中所有连接均采用 OpenSSL 库进行了加密,管理员的操作必须首先通过身份的验证[4]。

下面将从应用逻辑上结合图 1 与图 2 说明整个流程:

(1) 初始化认证中心。初始化完后,生成认证中心的自签名根证书和一份超级管理员证书。

(2) 超级管理员持自己的证书,通过 Windows 客户端程序连接认证中心,为政府采购管理员(具有政府采购业务中的最大权限)颁发个人证书,为政府采购管理网站颁发服务器证书(由于采用了 HTTPS 来访问)。图 1 中的 CA 代理可以使用超级管理员的证书,但从认证中心自身安全的角度看,超级管理员最好为 CA 代理颁发一张证书。

(3) 政府采购管理员凭自己的证书,通过 Web 浏览器以 HTTPS 登录政府采购管理网站,对地方管理员(地方政府财政人员)的资料进行审核,如果同意就为地方管理员设定相应的权限,并为地方管理员颁发一份个人证书;同时维护一些公众信息。

(4) 地方管理员同样凭自己的证书,通过 Web 浏览器以 HTTPS 登录政府采购管理网站,对地方供应商的资料进行审核,如果同意就为地方供应商设定相应的权限,并为地方供应商颁发一份个人证书;同时维护一些地方公众信息。

(5) 各地方供应商就可以凭自己的证书通过 Web 浏览器以 HTTPS 登录政府采购管理网站,执行相应的政府采购业务办理,并维护个人信息。

以上过程,除了认证中心的超级管理员采用的是 Windows 客户程序来颁发证书,其余所有的管理员均是采用浏览器来为下级颁发证书。

2.3 具体实现

2.3.1 认证中心(CA)的实现

认证中心在实现[5]上主要由三部分组成,分别是 CORBA 中间件服务、CA 服务程序(以 Linux 守候服务运行)和证书数据库,如图 3 所示。

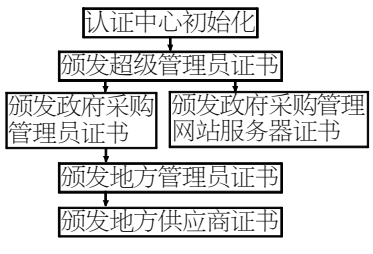

图 2 应用流程

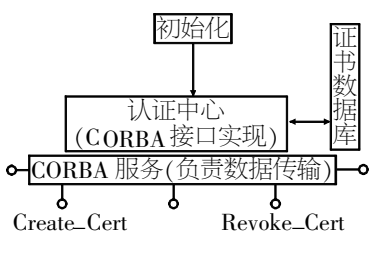

图 3 认证中心

CORBA 中间件负责与超级管理员客户端程序与 CA 代理之间的数据传输;CA 服务程序主要提供了生成证书、撤销证书、发布 CRL、恢复密钥、日志操作、认证中心的管理等 CORBA 服务接口[6],图 3 中标出了生成证书接口 Create_Cert 和撤销证书接口 Revoke_Cert,这些服务接口由接口定义语言[7](IDL)定义,采用 C++ 具体实现;证书数据库用来存放已颁发并被加密过的证书。所颁发的证书格式遵从 X.509 标准[8],密钥对的生成采用 RSA[9]算法。认证中心向用户提供两种格式的证书,即 PEM 格式和 PFX12[10]格式。

除了上面三个主要部分,认证中心还有一个初始化程序[11],认证中心程序在可以向外界提供服务之前,必须要有自己的根证书(自签名证书)。初始化程序作为一个交互式的控制台程序由超级管理员执行,超级管理员按照初始化程序的提示,输入认证中心根证书需要的内容项。初始化程序执行完后,将生成认证中心的根证书和一份超级管理员的个人证书。此后,认证中心服务程序将被启动,任何证书的生成将通过调用该服务程序完成,超级管理员也将通过 Windows 客户端软件进行对认证中心的操作。除非认证中心要更换根证书,否则初始化程序将不再执行。

2.3.2 政府采购管理网站实现

政府采购管理网站的主要功能是:向与政府采购业务有关的人员提供注册个人信息的功能;提供上级管理员向下级授权和颁发个人证书的功能;用户个人信息的发布。

在具体实现时,管理网站主要有以下五个部分:①网站 Web 服务器(Linux + Apache with mod_ssl + PHP);②注册信息数据库;③权限数据库;④CA 代理;⑤PHP 扩展模块。

以下是各部分的主要实现:

(1) 由于 Apache 中引入了 mod_ssl,浏览器访问时必须采用 HTTPS,所以就要将认证中心的根证书和超级管理员为该网站颁发的服务器证书一同拷贝到 Apache 的子目录 ssl.crt 中,并配置文件 httpd.conf,打开 SSL 的功能,指定前面两份证书的路径。

(2) 注册信息数据库保存用户初次录入的基本完整信息,包括姓名、单位等信息字段。

(3) 权限数据库中存放用户的证书与该用户的权限之间的绑定关系[12],主要的字段有:证书序列号(证书的唯一标志)、用户姓名、用户 E-mail、用户权限等。网站的各项操作都将参照此权限数据库。

(4) CA 代理主要是向 PHP 提供发放证书的功能。认证中心的功能很多,但与政府采购应用相关的功能主要是生成证书(认证中心的哪些服务由 CA 代理向 PHP 提供将由实际中的具体应用需求来作决定)。此外,CA 代理的存在,从某种程度上还可以对认证中心提供的服务进行一次“包装或过滤”后再提供给 PHP,增强了系统的灵活性。从认证中心的角度看,CA 代理是一个客户端;而从 PHP 的角度看,CA 代理又是一个服务端。在 Linux 平台上,CA 代理作为一个共享函数库模块存在,即.so 文件。

(5) PHP 扩展模块的功能主要是向 PHP 程序员提供生成

证书的导出函数,该导出函数的实现是通过调用 CA 代理所提供的生成证书的函数完成的。扩展模块的代码实现完全采用的是 Zend 提供的扩展模块编程规范。

图 4 演示了 PHP 扩展模块与 CA 代理的合作,共同完成基于 B/S 模式的证书发放实现。首先用户通过 Web 浏览器访问 Web 服务器,Web 服务器调用 PHP; 作为 PHP 的引擎——Zend 再去调用 PHP 扩展模块(该模块在 Web 服务启动时被加载到整个 PHP 当中) ; 然后, PHP 扩展模块去调用 CA 代理, CA 代理作为一个 CORBA 的代理服务端再去调用认证中心中生成证书的 CORBA 服务接口。结果沿逆序返回。

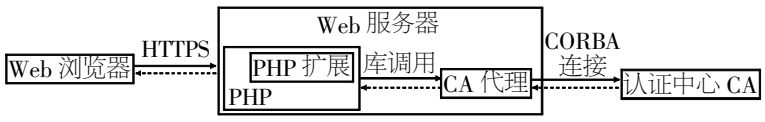

图 4　CA 代理与 PHP 扩展

2.3.3　超级管理员客户端软件的实现

超级管理员客户端软件的主要功能就是将运行在 Linux 平台上的认证中心的所有功能在 Windows 平台下提供给超级管理员一个良好的访问界面。类似 CA 代理,该客户端程序也是一个 CORBA 服务的客户端,只不过它映射了服务端的所有功能。超级管理员使用该软件进行对认证中心的操作,必须要有认证中心在初始化时为其生成的个人证书才可以通过身份认证。具体开发工具采用了微软的 Visual C++ 。

3　结束语

公钥基础设施(PKI) 有效地解决了网络安全中数据传输的保密性、完整性和不可抵赖等问题,更重要的是提供了密钥对发放的解决方案。本文所演示的就是利用 PKI 的如上优点,将 B/S 与 C/S 两种常见的应用架构结合起来,实现了一种证书发放的解决方案。该方案的实现可以满足目前众多基于 B/S 架构的电子商务、电子政务平台中所面临的权限访问控制这一重要需求,具有非常好的应用价值。

参考文献:

[1] 李涛. 网络安全概论[M] . 北京: 电子工业出版社, 2004.

[2] David W Chadwick. An X. 509 Role-based Privilege Management Infrastructure[EB/OL] . http: //sec. isi. salford. ac. uk/permis, 2002.

[3] PHP Manual[EB/OL] . http: //www. php. net/download-docs. php.

[4] 徐春林, 李涛, 张巍, 等. 基于 SSL 和 CORBA 技术的 CA 系统的实现[J] . 计算机工程与应用, 2003, 39(9) : 104-109.

[5] 张巍, 李涛, 徐春林, 等. 认证中心 FSCA 的设计与实现[J] . 计算机工程, 2003, 29(12) : 105-107.

[6] 张巍, 李涛, 刘晓洁, 等. 认证中心 CA 的功能及实现技术[J] . 计算机工程与设计, 2003, 24(9) : 38-39.

[7] Object Management Group. The Common Object Request Broker: Architecture and Specification[EB/OL] . http: //www. omg. org/oma, 2002.

[8] M Myers. Internet X. 509 Certificate Request Message Format[S] . RFC 2511, 1999.

[9] William Stallings. 网络安全基础教程——应用与标准[M] . 北京: 清华大学出版社, 2004.

[10] Pravir Chandra, Matt Messier, John Viega. Network Security with OpenSSL[M] . O'Reilly, 2002.

[11] 王伍戎, 李涛, 尹鹏, 等. 认证中心的设计与实现[J] . 网络安全技术与应用, 2001, (8) : 34-38.

[12] 鲜婷, 李涛, 等. 政府采购网站中的安全策略[J] . 网络安全技术与应用, 2001, (12) : 40-44.

作者简介:

黄锐(1981-) , 男, 河北人, 硕士研究生, 研究方向为网络安全与人工智能; 李涛(1965-) , 男, 四川人, 教授, 博导, 研究方向为网络安全与人工智能; 王姝妲(1982-) , 女, 四川人, 硕士研究生, 研究方向为网络安全; 王志明(1981-) , 男, 浙江人, 硕士研究生, 研究方向为网络安全; 丁勇雷(1981-) , 男, 江苏人, 硕士研究生, 研究方向为网络安全; 刘颖娜(1981-) , 女, 河南人, 硕士生, 研究方向为网络安全。

(上接第 112 页) 也可以实现从文到图的查询。我们可以采用 MapX 提供的 FindFeature 实现对象的查询。

```
//查询智能小区平面图中的停车场
CMapXFindFeature FoundObject = Map. GetLayers( ) . Item( "community" ) . GetFind( ) . Search( "park" ) ;
If ( FoundObject. GetFindRC( ) %10 = =1)
{
   m_Map. SetZoom( 100) ;
   m_Map. SetCenterX( FoundObject. GetCenterX( ) ) ;
   m_Map. SetCenterY( FoundObject. GetCenterY( ) ) ;
} else
   AfxMessageBox( "无相应查询结果." ) ;
```

3　结束语

GIS 技术用于智能小区物业管理系统开发大大提高了系统的交互性、可视化程度,便于智能小区物业部门的管理。将 MapX 控件和可视化的开发工具结合在一起可实现快速的组件重用,提高编程效率,有效地管理空间数据和属性数据。基于 MapX 的智能小区物业管理系统具有良好的应用前景。

参考文献:

[1] 刘光. 地理信息系统: 组件开发篇[M] . 北京: 中国电力出版社, 2003.

[2] MapInfo. MapX 5. 0 Online Help[EB/OL] . ftp: //betaftp. mapinfo. com/mapx/mapx50/MX5_Eval. exe, 2002.

[3] 夏红霞, 周宏, 杨红云, 等. 基于 GIS/GPS 车辆监控系统实现及关键技术[J] . 微机发展, 2004, 14(8) : 100-102.

[4] 周文生, 张子平. 住宅小区可视化物业管理系统的设计[J] . 计算机应用研究, 2000, 17(2) : 102-104.

[5] 史剑, 李军, 陈荦, 等. 基于 MapX 的空间查询应用[J] . 计算机工程与科学, 2004, 26(9) : 75-77.

作者简介:

钟珞(1957-) , 男, 湖南长沙人, 教授, 博导, 研究方向为软件工程、智能技术与智能系统、可视化技术; 李兵(1978-) , 男, 山东临沂人, 硕士研究生, 研究方向为软件工程、智能技术与智能系统、可视化技术; 夏红霞(1960-) , 女, 湖北武汉人, 副教授, 研究方向为软件工程、数据库与信息处理; 徐俊杰(1982-) , 男, 湖北随州人, 硕士研究生, 研究方向为计算机网络与软件工程。