基于 PKI 技术的认证中心研究

李 彦 王柯柯

(重庆工学院网络信息中心 重庆 400050)

摘 要 PKI技术是目前能够有效地全面解决安全问题的可行方案,本文重点讨论了 PKI 的核心——CA 认证中心,提出了企业级认证中心的设计思路,并详细地描述了该 CA 的总体结构和设计模型。

关键词 PKI,CA,数字证书

The Research of the Corporation-Rate Certificate Authority

LI Yan WANG Ke-Ke

(Network&Information Center, Chongqing Institute of Technology, Chongqing 400050)

Abstract Now, The PKI technology is a feasible project of solving the safe problem effectively. The article discusses the PKIs nucleus——CA, and expounds the corporation-rate CA's design way, and carefully recounts the CA's ensemble structure and device model.

Keywords Public key infrastructure, Certificate authority, Digital certificate

在信息安全技术领域里,公开密钥加密技术近年来发展很快,在这项技术的基础之上形成和发展起来的公开密钥基础设施 PKI(Public Key Infrastructure)很好地适应了互联网的特点,为互联网以及相类似网络应用提供了全面的安全服务。因此,利用 PKI 技术提供的平台、服务和解决方案来保障网络应用的安全实施是十分必要的。

电子政务及电子商务目前发展迅速,为了配合政府机关和企业的信息化工作,增强网上操作的安全性,为其构建提供安全身份认证的数字证书认证中心 CA(Certificate Authority)迫在眉睫,以保障关键数据的传输安全和实现电子身份认证。本文就是基于 PKI 技术,提出了企业级认证中心的设计思路,详细讨论了该 CA 的总体结构和设计模型。

1 公开密钥加密算法 RSA[1]

公开密钥加密算法(public-key algorithm)又称非对称密钥加密算法,它之所以被称为非对称的,是因为进行加密和解密操作所使用的并不是同一个密钥而是两个不同的密钥:一个是公钥(public-key),通常用来加密信息,一个是私钥(private-key),通常用来解密信息(但有时也会交换使用);它之所以又被称为公开密钥算法,是因为加密密钥能够被公开,其他人可以用这个公开的密钥来加密信息,但只有用相应的解密密钥才能进行解密。

非对称密钥加密算法中,RSA 算法是最为成功的。它采用足够大的整数,原因是因子分解越困难,密码就越难以破译,加密强度就越高。RSA 算法的密钥管理比较简单,可以较方便地实现数字签名和验证,但是算法复杂,加密效率较低,因此,在实际应用中通常不采用这一算法对大数据量的信息进行加密。

下面来描述一下 RSA 算法的具体实现步骤:

- 公开密钥:$n = pq$(p,q 分别为两个互异的大素数,p,q 必须保密)
- 公开密钥 e 与 $(p-1)(q-1)$ 互素;
- 秘密密钥:$d = e^{-1} (\mathrm{mod}(p-1)(q-1))$;
- 加密:$c = m^e (\mathrm{mod}\ n)$,其中 m 为明文,c 为密文;
- 解密:$m = c^d (\mathrm{mod}\ n)$

2 PKI/CA 理论[2]

公钥基础设施提供了一个框架,使你可以在这个框架下实施基于加密的安全服务。它是一个基础设施,利用非对称密码算法的原理和技术来实现,提供安全的服务并且具有通用性的安全,它为电子商务、电子政务等的顺利开展提供一整套安全的基础设施。PKI 的核心是认证中心 CA,所以通常称为 PKI/CA。

2.1 数字签名

数字签名类似于使用手签字和印章的文件,它可以保证文件内容没有被改变,文件出自签字人之手或经过签字人批准,以此来保证信息传输过程中信息的完整性以及提供信息发送者的身份认证和不可抵赖性。目前,数字签名技术的研究主要是基于公钥密码体制来实现,有两个密钥:一个是签名密钥,必须保持秘密;另一个是验证密钥,它是公开的。

要生成数字签名,信息的发送方需使用单向 Hash 函数将信息 M 压缩到某一固定长度的信息摘要(Message Digest),在数学上要保证只要改动报文中任何一位,那么重新计算出的报文摘要值就会与原先的不相符,以保证不可更改性。再用自己的私钥对这个摘要进行加密来形成发送方的数字签名。要验证数字签名,信息发送方首先生成信息的数字签名,然后将这个数字签名作为信息的附件和信息一起发送给接受方;信息的接受方首先从接受到的原始信息中计算出信息摘要,然后再用发送方的公钥来对信息附加的数字签名进行解密,如果两个 Hash 值相同,那么接受方就能够确认该信息是发送方发送的。

2.2 数字证书

李 彦 硕士,研究方向:计算机网络,信息安全分布式计算;王柯柯 硕士,研究方向:计算机配件工程,计算机网络安全。

数字证书的作用类似于现实生活中的身份证，由一个权威机构发行，在一个身份和该身份的持有者拥有的公/私密钥对之间建立了一种联系，人们可以在通讯的过程中用它来识别该身份。如果你想要确立身份，那么你可以信赖一个特定的颁发机构，由这个机构根据你要达到的目的来确立，然后就要生成一份可以证实你已经获得了一个有效身份的文件，而数字证书就是这么一文件的电子形式。有了数字证书，就可以使得别人能够说服他们自己相信你就是该身份的合法的持有者。

目前定义和使用的证书有多种，而大多数使用的都是 X.509 v3 公钥证书，其属性有：

Certificate Format Version(版本号)

Certificate Serial Number(证书序列号)

Signature and Hashing Algorithm for the CA

(CA 用来签发证书使用的签名和 Hash 算法)

Issuer Name(颁发者)

Validity Period(证书有效期)

Subject Name(主体名)

Subject Public Key Information(申请者公钥信息)

Issuer Unique Identifier(证书签发者唯一标识符)

Subject Unique Identifier(证书申请者唯一标识符)

Type Criticality Value Extension(扩展项类型、关键标志、扩展项值)

CA Signature(CA 对该证书的数字签名)

2.3 认证中心 CA

认证中心 CA(Certificate Authority)是 PKI 框架中唯一能够发布和撤销证书的实体，它为每个使用公开密钥的用户发放一个数字证书，以证明证书中列出的用户名称与证书中列出的公开密钥对应，当用户身份和各项相关信息通过注册中心(RA)审核后给用户颁发证书，使证书持有者和持有者公/私密钥对、相关信息与证书中心建立一种联系，是网上交易的用户的客观真实性与证书的真实性一致。

CA 的功能包括：证书的申请、证书的审批、证书的颁发、证书的作废、证书的在线查询更新及 CRL 的发布和管理等等，它可以按照一定的信任模型来组织，如层次模型、分布式模型或 Web 模型等，本论文讨论的 CA 所采用的是严格层次信任模型，严格层次结构可以描绘为一棵倒转的树，根在顶上，树枝向下伸展，树叶在下面。在这棵倒转的树上，根代表一个对整个 PKI 域所有实体都有特别意义的 CA，通常叫做根 CA，作为信任的根或“信任锚”，它是最可信的证书权威，所有其它信任关系都起源于它。在这个模型中，层次结构的所有实体都信任唯一的根 CA。

3 企业级认证中心的设计

3.1 CA 中心总体结构

CA 系统的总体设计采用了层次结构，并根据证书链的扩展能够支持 CA 发展多层下属子 CA，从应用上安全可靠的支持多种电子商务模式(B TO C，B TO B 等)，所采用的技术标准和接口规范都符合国际标准，能够方便地与其它国家和地区以及行业的认证中心进行交叉验证，扩大信用范围，为在更广范围内开展电子商务活动提供了可能[3]。

本 CA 中心的总体框架设计为三层结构，即根 CA、第二层 CA 和底层 RA，这样设计的目的是加强对根 CA 签发证书密钥的保护，如图 1。

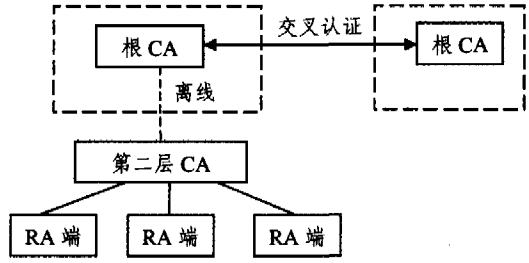

图 1 CA 的总体结构

本证书认证中心的根 CA 设计为离线操作，它覆盖范围为整个企业内部，将来进一步发展，可利用此根 CA 与其它行业的 CA 进行交叉认证以支持更大范围的认证；第二层 CA 作为直接接受用户申请的操作界面，为广大的终端用户提供服务和支持，它需要经常发放证书并且需要迅速响应，所以必须在线操作；最终用户向证书注册机构 RA 申请登记，RA 就向通过申请的用户发放由第二层 CA 提供的参考号和授权码，用户通过它们就可以得到证书。

3.2 CA 的设计模型

在设计企业级 CA 认证中心的过程中，我们充分考虑了系统的特点及系统未来的可扩充性，提出的设计模型如图 2 所示。

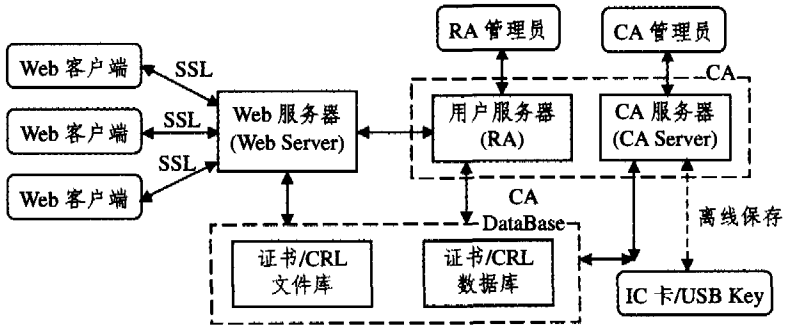

图 2 CA 的设计模型

用户在申请证书之前，必须事先安装自己信任的 CA 的根证书，这样才能拥有 CA 的公钥来进行验证。

首先，用户在自己的客户端生成公/私密钥对，通过 Web 客户端的浏览器界面填写好证书信息，将公钥和证书信息生成证书请求信息 CRS，发送给 Web 服务器，向系统提出申请。Web 服务器将此申请发送给 RA，由 RA 管理员通过 RA 服务器的管理员界面审核用户的申请，若申请通过，则将此申请

(下转第 148 页)

录取人数、最高分、最低分及其分布等。可以根据新生入学管理的需要自定义查询条件和自定义字段等导出相关数据。可以将以上导出结果自动生成 Excel 或 Dbf 格式的文件。

由于各高校的录取通知书每年设计均不相同，数据处理系统还可以自定义每个字段内容的打印位置，并能选择激光打印机或针式打印机打印通知书和信封，具有智能打印通知书和信封的功能。

2.2 Web 查询系统设计

录取结束后，经过数据处理系统对录取新生的数据进行处理，考生即可通过 Web 查询系统查询录取结果。查询方式是通过考生考号精确查询，或通过准证考号和省份精确查询，如已录取，则显示考生录取的院系、专业、邮寄通知书详细地址等信息。

2.3 现场信息处理系统设计

现场信息系统可以通过省份、院系、专业、考生号、姓名等查询条件模糊组合查询考生录取情况，可以复现考生详细电子档案，包括考生信息、成绩与志愿、体检信息、考生报名表、体检表和附加表等。可以模糊查询退档考生的信息和退档原因。另外可以实时统计各院系、各专业的男女学生录取人数等。

3 招生录取管理系统的应用

招生录取管理系统部署时需要配置一台服务器，设置好 IIS，SQLServer2000 可直接安装在服务器上，也可安装在其他计算机上。现场信息系统可配置在局域网中，Web 查询界面配置在公网上。

根据实际需要，后台数据库也可采用 Orcale，现场信息系统的功能可作进一步扩展，如根据授权，让院系直接查询本院系新生电子档案信息等。

招生录取管理系统既可独立使用，为学校后续管理提供新生数据，也可直接和高校实施的数字化校园接口，调用公共数据库的相关表和生成新生数据等。

结束语 通过对“全国普通高校招生管理系统”系统进行深入分析，进一步设计了招生录取管理系统，经过 4 年的试用和完善，能达到有效提取、复现学生电子档案数据，完善了招生录取管理、新生入学管理等基础性信息服务，大大提高了招生录取时数据处理的效率，及时打印寄发录取通知书，让考生快速查询到自己的录取情况，为教育部推行的“阳光招生”作了最好的技术保障。同时为高校数字化校园项目中学生基础电子数据库的形成奠定了良好的基础。

参 考 文 献

1 教育部高校学生司，清华大学计算机系. 全国普通高校招生网上录取系统院校使用手册. 2001-06

2 吴洪潭，叶含笑，丁文. 高校网上招生系统院校端子系统的设计[J]. 计算机工程[增刊]，2002，28：287～290

3 王刚，杨风和，陈世福. 基于分布式对象技术和 MTDAS 的普通高校网上招生系统-院校端辅助子系统[J]. 计算机与网络，2004，4：57～59

4 异构数据库之间的导入导出示例[EB/OL]. http://www.delphi-fans.com/InfoView/Article_7.html，2004

5 张升平，陆渝. 用 Delphi 开发安全强固的多层分布式数据库应用系统[J]. 重庆工商大学学报(自然科学版)，2003，20(1)：41～43

(上接第 111 页)

存入数据库。当 CA 管理员通过 CA 服务器的管理员界面进入数据库中查询到有已通过申请的用户时，CA 管理员就是要使用 CA 的私钥对 CRS 进行签名，生成用户的数字证书，并保存在证书/LDAP 数据库中，为安全起见，需要将证书离线保存入 IC 卡或 USB Key 中。此时，用户可以在线下载自己的证书文件，并和自己的私钥放置在一起，并且用户可以登录 Web 服务器的界面查询某一证书的相关状态。当用户请求废除证书的时候，CA 管理员提出保存在数据库中的请求，经过确认后，直接将证书的唯一序列号填入 CRL，定时发布 CRL。

针对以上的设计模型，我们还考虑了几点细节：

• 用户密钥对的产生：在 RFC2510 中对申请证书时产生公开密钥对的地点有两种方案，一是由 CA 集中生成；二是由用户在本地生成。我们考虑到用户私钥的安全性，采用第二种方式，由 CA 的证书申请端借用系统动态连接库 Xenroll 的密钥生成函数，在用户本地机上生成密钥对，其中私钥保留在网络浏览器的密钥容器中，公钥部分交由 RA 申请证书。

• RA 和 CA：为了保证系统的安全性和可扩展性，采用 RA 和 CA 相分离的管理模式，并提供必要的 RA 接口，如果随着系统的扩展需要开发完整的 RA 审核功能模块，只需在现有系统中挂接一个新的功能增加完整的 RA 模块，无需对系统的其他部分进行任何改动，同时又满足了用户目前对于系统简单易用的要求。

• 备份服务器：为了保障用户证书和公钥的安全性，在证书数据库之外还增加了一个备份服务器来存放用户的公钥和为用户生成的数字证书。当用户需要更新或撤销证书时，CA 必须将备份服务器中的证书同时更新或撤销。

结束语 该企业级认证中心可广泛适用于各种基于 WEB 的应用系统，如网上招投标系统、网上银行、网上采购等等，对于敏感数据传输安全、身份认证等安全问题，基于 PKI 技术的 CA 认证中心能够比较好地解决。本文讨论了 PKI/CA 的相关理论，提出了企业级认证中心的设计思路，并对该 CA 的总体结构和设计模型进行了详细的描述，在理论和应用上都有广阔的前景。

参 考 文 献

1 卿斯汉. 密码学与计算机网络安全[M]. 北京：清华大学出版社，2001

2 关振胜. 公钥基础设施 PKI 与认证机构 CA[M]. 北京：电子工业出版社，2002

3 尹鹏. 认证中心的设计与实现[D]. 四川：四川大学计算机学院，2001

4 Stallings W. 密码编码学与网络安全[M]. 北京：电子工业出版社，2001

5 肖凌，李之棠. 公开密钥基础设施(PKI)结构. 计算机工程与应用，2002，38(10)：137～139