

一种自助型证书授权认证中心的设计

李 新

(中国科学院 计算机网络信息中心, 北京 100080)

(ca365@sohu.com)

摘 要:证书授权(Certification Authority, CA)的价值表现在权威和技术两个方面,典型的 CA 认证中心为保证 CA 的权威性花费了巨大的建设和运营成本。企业应用的特点决定了企业 CA 可以适当放弃 CA 的权威性而重点利用 CA 的技术来解决应用系统的安全问题,自助型 CA 就是针对企业应用系统的具体情况对 CA 的简化。在自助型 CA 认证中心中,没有 RA(Register Authority)和独立的证书库,只保留 CA 服务器,可以随时签发证书,并且与企业应用的访问控制系统融为一体,使用方便,建设和运营成本很低。

关键词:证书授权;公钥基础设施;自助

中图分类号: TP309 **文献标识码:** A

Design of a kind of self-help certification authority

LI Xin

(Computer Network Information Center, Chinese Academy of Sciences, Beijing 100080, China)

Abstract: The value of CA depends on two aspects, authority and technology. Ordinary CA costs most on construction and maintenance in order to insure its authority. Enterprise CA can decrease its authority and focus on utilization of its technology to deal with security problems in application system because the character of enterprise application. Self-help CA is just a type of simplified CA that adapted to enterprise application. Self-help CA disposes RA and independent certificate database only reserve CA Server and can sign certificates at any moment. Self-help CA can be integrated with access control system of application and is easily used, cost in construction and maintenance is lower.

Key words: Certification Authority(CA); PKI(Public Key Infrastructure); self-help

0 引言

近几年,作为信息安全的一项主流技术,CA(Certification Authority)得到了广泛的应用,许多行业及地方都建设了自己的 CA 认证中心,以 CA 为核心的应用技术(如:电子印章、签名/加密、身份认证)不断涌现,为网上安全电子交易提供了有力的技术保障。CA 已经成为电子商务安全技术的事实标准,并且开始应用到企业信息化领域。

然而,当人们将电子商务中 CA 建设的成功经验应用于企业信息化时,却不得不面对 CA 认证中心昂贵的建设和运营成本,动辄上千万的建设费用和烦琐复杂的管理流程,成为制约 CA 在企业中推广应用的瓶颈。因此,能否简化 CA 认证中心的技术构架和管理流程,降低 CA 的建设和运营成本,使 CA 成为中小企业能够消费得起的技术,是 CA 在企业信息化中能够顺利推广的关键因素之一。

1 典型的 CA 认证中心及应用

CA 最早应用于电子商务领域,最初的目的是要解决电子交易双方的身份确认问题,由于网上电子交易双方远隔千里、互不相识,确定交易者身份的过程十分严格复杂^[1~4]。

一个典型的 CA 认证中心包括 CA 服务器、注册中心 RA(Register Authority)和相应的证书存储库。CA 服务器是认证中心的核心,负责处理来自 RA 的证书签发和吊销申请;注册

中心 RA 负责接受用户的证书注册和吊销申请,对用户的真实身份进行审查,并决定是否向 CA 提交签发或吊销数字证书的申请;证书存储库用于对 CA 签发的证书和证书吊销列表 CRL 等信息进行存储和管理,并提供相应的查询功能,典型的证书库一般采用 LDAP 服务器。

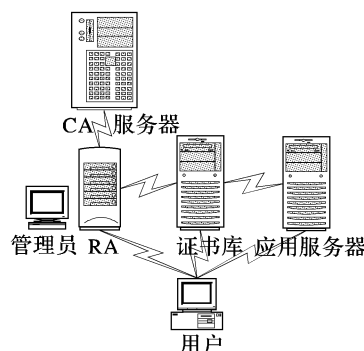


图 1 典型的 CA 认证中心及应用系统

为了保证 CA 认证中心签发的证书安全有效,CA 服务器必须置于高度安全的环境下,RA 对用户身份的验证必须有严格的人工参与审核。证书库只提供证书及 CRL 的查询功能,在 CA、RA 高度安全的前提下,可以选择较低的安全级别,因为无论证书还是 CRL 都包含 CA 根证书的数字签名,具有严格的不可伪造性,伪造的证书库信息很容易被用户识别,因此,证书库只要确保正确证书及证书吊销列表能够没有遗漏

的被检索到即可。

在典型的 CA 认证中心的支持下,应用系统利用证书确定用户身份十分简单,只需要经过两个步骤就可以确定用户身份:首先让用户对一段随机数进行数字签名,验证用户签名的有效性,以确定用户持有相应密钥;然后访问证书库,确定用户证书是否有效,并根据证书主题内容确定用户身份。图 1 为一个典型的 CA 认证中心及应用系统的系统结构图。

2 企业信息安全的特点

CA 的价值反映在权威和技术两个方面。CA 的权威性保证 CA 签发的证书能够反映证书持有者的真实身份,即证书的主题内容与用户的真实身份一致;CA 的技术性保证用户所操作的数据具备完整性、可靠性、机密性等特点。为了保证 CA 的权威性,典型的 CA 认证中心花费了大量的建设和运营成本,而 CA 的技术性由签名/加密算法的可靠性来保障,成本较低。

在企业应用中,CA 认证中心的建设应该根据企业自身的特点,选择合适的策略,以简化系统结构,避免不必要的浪费。

首先,企业应用系统中的用户一般局限在企业自身的员工范围内,并不像电子商务的用户那样远隔千里、彼此陌生,严格复杂的身份审核工作并不必要。

其次,根据证书主题来判断用户身份的做法在企业应用中并不实用,这主要表现在以下几个方面:

1) 企业应用系统中的用户往往具有多重身份,现实中一人身兼数职的情况十分常见,一人一个证书难以满足应用系统需求,而允许一人持有多个证书则会给用户带来不必要的麻烦。

2) 企业中的组织机构关系复杂,常常存在一个机构同时隶属于两个不同的上级机构管理的情况,甚至还会出现同一个机构在不同的子系统中隶属关系不一致的情况,因此,仅靠证书主题及 LDAP 简单的树型结构,无法反映现实中的复杂情况。

3) 企业应用系统一般都有一套自己管理的组织机构及用户、角色、权限管理系统,这样的管理系统一般都建设在关系型数据库中,能够处理各种复杂情况,企业应用系统往往更习惯采用自己的管理系统判断用户身份,而不是根据证书主题来判断。

4) 在典型的 CA 认证中心运营模式下,当组织机构或用户身份发生改变时,需要 CA 认证中心吊销旧证书并重新签发新证书,过程十分繁琐,尤其是对于人事变动频繁的企业。

因此,在证书主题信息及 LDAP 无法满足企业应用的情况下,企业引入 CA 后,应用系统仍然需要采用自身的组织结构及用户、角色、权限管理系统判断用户身份。验证用户身份时,证书的作用仅仅是替代用户名/密码。

企业 CA 建成后,原有系统的改造十分容易,只要在包含用户名/密码的数据表中增加存放数字证书字段即可。当用户登录时,不再比较用户名/密码,而是比较用户签名证书的公开密钥与数据表中存放的用户数字证书的公开密钥,依此判断用户身份。

3 自助型 CA 认证中心的设计

由于应用系统判断用户身份没有采用证书主题提供的信息,因此,典型 CA 在证书签发过程中为保证 CA 认证中心的权威性所花费的建设和运营成本,在企业 CA 中并不必要。

数字证书通过公开密钥与用户表中的记录相关联,证书主题的内容与应用系统中用户的实际身份没有任何关系。在企业 CA 认证中心的系统结构中,可以省略典型 CA 认证中心中注册中心 RA 为审核用户身份所做的工作,由于应用系统用户表中保存了数字证书,单独的证书库也不再需要。因此,企业 CA 认证中心可以简化为一个简单的 CA 服务器,CA 的运营也可以采用“自助”的方式。

图 2(a) 为一个自助型 CA 服务器及应用系统。申请证书时用户直接向 CA 服务器提交申请,密钥对在客户端产生,用户只向 CA 服务器提交包含公共密钥的证书申请文件,整个过程没有任何途径的私钥传播,私钥的安全性得到保障。CA 服务器直接接受用户的证书申请并签发证书,CA 在签发证书时并不验证用户的真实身份,任何申请都签发,来者不拒。用户得到证书后自己将证书上传到应用服务器,存放到用户表中的证书字段,就可完成从用户名/密码向证书的转换和证书的定期更新工作,整个过程不需要管理员的参与。

由于判断用户身份根据的是用户表中的证书公开密钥,而非证书主题,因此,证书的吊销也不再必要。当用户身份改变时仅仅改变应用系统中的组织机构和用户表间的关系即可,并不影响旧证书的使用;当证书密钥失窃时,也不必吊销证书,用户自己重新申请一个证书即可。因此在自助型 CA 认证中心的运营模式下,可能发生频繁人事变动或具有多重身份的用户在申请证书时,可以填写自然人的主题信息而非组织机构主题信息。

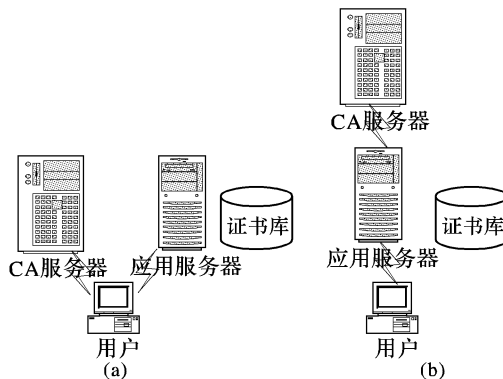


图2 自助型 CA 服务器及应用系统

4 针对签名和加密的改进

认证用户身份只是数字证书功能的一部分,有时应用系统需要利用数字证书对数据进行签名或加密^[5]。自助型 CA 认证中心由于放弃了 CA 的权威性,在实现数据的签名或加密时,有一定限制。

签名采用的是签名人的私钥,验证签名时采用签名人的公开密钥,在验证签名时除了验证数据是否完整外,更重要的是要知道签名人的详细信息。典型的 CA 认证中心签发的证书能够保证证书主题内容与证书持有人的真实身份一致,因此可以将证书与签名数据捆绑在一起,签名数据离开应用系统后仍然可以验证签名的有效性。自助型 CA 无法保证证书主题内容的真实性,因此将证书与签名数据捆绑在一起没有意义,只能通过系统本身的用户表判断签名人的真实身份,这种签名无法离开系统独立使用。

加密采用的是对方的公开密钥,密文数据只能用对方的私钥解密,加密时为了保障数据安全,有时需要验证一下对方

(下转第 1323 页)

无法使用系统。在系统运行过程中,此模块动态监控 IC 卡状态,一旦用户抽掉 IC 卡,系统立即能够识别,停止运行,保障了系统运行过程中的用户身份安全。同时,IC 卡内用户密钥信息采用加密方式存储,即使遗失,由于不知道用户口令,也无法获取。通过以上方式,能有效防止攻击者的假冒合法用户身份的攻击。

2) 用户主密钥是在发卡时由伪随机序列产生,并以用户口令为密钥加密存储于智能卡中。只有在智能卡 and 用户口令都具备的情况下,才能成功获取主密钥,二者缺一不可。攻击者很难通过字典式口令猜测攻击等非法手段得到用户主密钥。

3) 在对用户身份进行认证时使用认证服务器生成的随机会话密钥,而不是使用用户口令做为密钥。从而避免攻击者使用非法手段获取用户口令,获得会话密钥。并且随机会话密钥只用于本次会话,只在本次会话有效,有效时间很短。即使攻击者采用离线攻击方式窃取了会话密钥,但当会话密钥失效后也无法冒充合法用户。

4) 在终端对服务器发出门票请求消息后,服务器生成随机数,并以会话密钥加密后做为挑战发送给对方。终端只有在返回正确的随机数后,服务器才通过对终端的身份的确认。使用这种挑战/响应的方法,解决了 kerberos 协议中存在的基于时间戳的鉴别符不能有效防止重放攻击,且分布式系统很难维持比较精确的时间同步的弱点。

5) 认证服务器的安全得到保证,并易于维护。记录用户信息的数据库中,用户对应主密钥采用加密方式存储,攻击者即使能访问数据库,但因为无法获得认证服务器对应主密钥,也无法窃取合法用户信息,认证服务器的安全得到保障。在每一次身份认证过程中,与终端一次通信所需的全部有用数据均保存在 TGT 中,包括用户名、会话密钥、门票过期时间等等。认证服务器只需解密 TGT 即可获得此次通信所需全部信息。这样可使认证服务器无须进行状态维护,也不需要存储任何临时数据,只需要有一个记录合法用户信息的静态数据库,从而减轻认证服务器的负担,很容易地实现认证服务器的维护。

(上接第 1319 页)

的真实身份。对于典型的 CA 认证中心签发的证书,可以用证书主题信息作为判断对方真实身份的可靠依据。而对于自助型 CA 认证中心,只能从系统的用户表中提取对方信息。相对与典型的 CA 认证中心严格的身份审核机制和高度安全的网络环境,应用系统的安全可靠性要差得多,因此,用自助型 CA 签发的证书进行签名/加密,有一定的安全风险。

为了弥补自助型 CA 认证中心签发证书的随意性带来的安全隐患,图 2(b) 对自助型 CA 认证中心进行了一定的改进。改进后的 CA 服务器不再直接面对用户接受申请、签发证书,而是运行在应用服务器后台,用户通过应用服务器身份认证后才能申请证书。证书主题的内容也不再是用户随意填写,而是由应用系统从用户信息表里自动提取。用户信息表中的用户身份关键数据(如:用户姓名、所属部门、职位等),只能由有特殊权限的管理员填写,普通用户不能直接更改。这样可以在一定程度上保证证书主题的可靠性,从而提升自助型 CA 认证中心的权威性。

5 结语

相对于典型的 CA 认证中心,自助型 CA 认证中心的建设

6) 在终端和 MCU 身份认证过程中生成的用于终端和 MCU 之间进行通信的会话密钥,除了用于终端和 MCU 相互进行认证外,还可用于终端和 MCU 在 H. 245 通信过程中产生的媒体流会话密钥的加密密钥,无须另外再次生成密钥,提高系统效率。

7) 系统对用户身份认证基于 Kerberos 协议,Kerberos 采用对称加密算法,运算速度比公钥算法高出百倍,效率很高,能满足视频会议系统对实时性要求较高的特点。

3 结语

视频会议系统中的身份认证问题是视频会议系统安全最基础也是最重要的保障。本文提出的一种视频会议系统身份认证的解决方案,利用智能 IC 卡对用户身份进行识别,不仅在通信开始前对用户身份的识别,还能在系统运行过程中动态监控用户身份变化。利用改进的 Kerberos 实现对视频会议系统用户身份的认证,能有效防止攻击者的各种攻击,并解决了 Kerberos 协议存在的缺陷,安全性好。同时能满足视频会议系统对实时性要求较高的特点,是一种非常适合视频会议系统特点的身份认证解决方案。

参考文献:

- [1] ITU-T Recommendation H. 323. Packet-Based Multimedia Communications Systems[S], 1998.
- [2] ITU-T Recommendation H. 235. Security and encryption for H-Series (H. 323 and other H. 245-based) multimedia terminals[S], 2000.
- [3] BELLOVIN SM, MERRITT M. Limitations of the Kerberos Authentication System[J]. Computer Communications Review, 1990, 20(5): 119-132.
- [4] NEUMAN BC, TS' O T. An Authentication Service for Computer Networks[A]. IEEE Communications Magazine[C]. September, 1994. 33-38.
- [5] STALLINGS W. 密码编码学与网络安全:原理与实践[M]. 第2版. 北京:电子工业出版社, 2001.
- [6] 刘玉,徐一新,王长强,等. 机要公文安全分发的一种解决方案[J]. 华中科技大学学报(自然科学版), 2003, 31(8): 102-104.

和运营成本大大降低,但是这种成本的降低是在牺牲 CA 认证中心的权威性的前提下取得的。自助型 CA 认证中心在结构上与企业应用系统融为一体,具有简单、方便的特点。

考虑企业应用的具体情况,很多时候对 CA 认证中心的权威性的需求并不显著,这时,采用自助型 CA 认证中心颁发数字证书,可以充分利用 CA 的技术为企业的信息安全提供保证。

参考文献:

- [1] 袁卫忠,王德强,茅兵,等. 公钥基础设施的研究与进展[J]. 计算机科学, 2004, 31(2): 82-88.
- [2] 孟桂娥,董邦文,杨宇航. 公钥基础设施 PKI 的设计[J]. 计算机工程, 2001, 27(6): 111-113.
- [3] 金晓秋,郭巍,金亿平,等. PKI 中的证书和发证机构[J]. 计算机科学, 1999, 26(7): 83-86, 76.
- [4] 李新,孙玉芳. 基于关系型数据库的 CA 系统[J]. 计算机工程, 2004, 30(8): 1-3.
- [5] 李新,张继东,孙玉芳. 签名加密技术在公文系统中的应用[J]. 计算机应用研究, 2004, 21(4): 98-99.