公钥基础设施的研究与进展*)

袁卫忠　王德强　茅　兵　谢　立
(南京大学计算机软件新技术国家重点实验室　南京210093)

摘　要　随着电子商务和电子政务的发展,公钥基础设施作为安全基础设施,在信息系统安全中起着重要作用。虽然公钥基础设施获得了快速发展和部署,但仍存在许多风险和问题有待解决,以满足信息安全的新需求。在本文中,我们介绍分析一些新的PKI解决方案、服务、技术,以及第二代PKI技术。

关键词　公钥基础设施,认证中心,证书,XML密钥管理规范

Survey of Public Key Infrastructure

YUAN Wei-Zhong　WANG De-Qiang　MAO Bing　XI Li
(Department of Computer Science and Technology, State Key laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)

Abstract　With the development of e-commerce and e-government, Public Key Infrastructure (PKI) has played an important role in the information system security as a security infrastructure. Although PKI has been developed and deployed rapidly, there're still many risks and problems to be solved to meet the new requirements of the information security. In this paper, we introduce and analyze some new solutions, services and techniques of PKI, including the techniques of the secod generation PKI.

Keywords　Public key infrastructure, Certification authority, Certificate, XML key management specification

1. 引言

公钥基础设施(Public Key Infrastructure,PKI)就是一个用公开密钥(简称公钥)概念和技术实施和提供安全服务的具有普适性的安全基础设施。PKI是信息安全技术的基础和核心,也是电子商务、电子政务的关键。PKI系统中的认证中心(Certification Authority,CA)作为证书颁发权威,为其所颁发的数字证书提供用户身份和公钥信息间绑定的认证。PKI本身支撑的安全服务才是用户所真正需要的,并与之接触的,这些服务建立在PKI核心服务基础上。

到目前PKI技术已经研究了十多年,但仍然面临一些风险和困难。同时,由于标准的制定组织比较多,并且受到主要实施厂商的影响,缺乏一个被全球广泛接受的互操作性标准,不同PKI系统之间很难取得互操作性。本文将对PKI最近几年内出现的主要技术和方法予以介绍分析总结。本文第1节以下部分对PKI系统基本标准、信任模型和组成部分等进行系统介绍;第2节从PKI体系结构层次进行介绍分析;第3节对新PKI服务技术进行介绍分析,第4节对PKI系统总体需求层次进行介绍分析,第5节介绍PKI仍然存在的风险和问题,最后是结束语。

1.1　PKI系统概述和体系结构

PKI是一个包括硬件、软件、人员、政策和手续的集合,用来实现基于公钥密码体制的公钥身份证书产生、管理存储、发行和作废等功能。它使众多的CA具有一个开放性的标准,使CA之间能够互联、互相认证,以及实现一个安全的CA管理、应用体系。

在PKI中,把一般普通证书用户称作为终端实体(End Entity,EE),以和认证中心、注册机构等PKI管理实体区分开来。认证中心负责数字证书和证书作废表(Certificate Revocation List,CRL)的颁发,CRL又被称作证书黑名单。CA可把用户注册审核工作授权给一个可选的机构—注册机构(Registration Authority,RA)来完成。终端实体向注册机构提交证书申请,注册通过后由认证中心为终端实体颁发数字证书,并将数字证书发布到证书库中。认证中心还可以把自己颁发CRL的功能授权给独立的CRL颁发者来完成,CRL也被发布并存储在证书和CRL库中。终端实体可以到证书和CRL库中检索、下载所需要的证书和CRL。另外,CA还能给其他CA颁发数字证书,或根CA(Root CA)相互之间进行交叉认证。图1是IETF的PKIX工作组所提出的PKI简化模型图[1]。

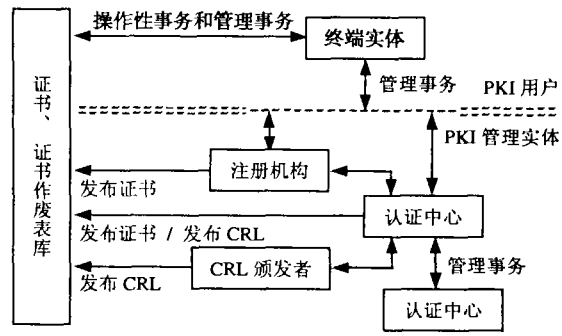

图1　PKI实体关系图

*)本课题得到江苏省"十五"科技重点攻关项目(BG2000006)和(BE2001065)资助。袁卫忠　博士研究生,研究方向为信息系统安全。王德强　博士研究生,研究方向为信息系统安全。茅　兵　教授,研究领域为信息系统安全,分布式操作系统等。谢　立　教授,博士生导师,研究领域为信息系统安全,分布式操作系统等。

1.2 PKI 各组成部分和技术要点

现在应用对 PKI 的总体需求可以概括为双密钥对、双中心模式。

双密钥对模式：公钥的两大用途是用于验证数字签名和用于加密信息。相应地，系统中需要配置用于数字签名/验证的密钥对和用于数据加密/解密的密钥对，这里分别称为签名密钥对和加密密钥对。(1)签名密钥对由签名私有密钥(简称私钥)和验证公钥组成。在电子签名法案通过后，签名私钥具有日常生活中公章、私章和手写签名的效力。用作数字签名的这一对密钥一般可以有较长的生命期。(2)为防止密钥丢失而造成丢失数据，加密密钥对的解密私钥应该进行备份，同时还需要进行存档，以便能在任何时候解密历史密文数据。加密密钥对的生命周期较短。这两对密钥对的密钥管理有不同的要求，存在互相冲突的地方，因此，PKI 必须针对不同密钥用途使用不同的密钥对，即至少需要使用两对密钥对，这被称作双密钥对模式。

双中心模式：认证中心 CA 和密钥管理中心(Key Management Center，KMC)被称为双中心。KMC 的存在有如下两个理由：①为确保加密数据的可用性，双密钥对中的加密密钥对应该被备份，并在需要的时候能被恢复(也称为密钥托管，Key Escrow)；②为了打击犯罪分子利用密码技术进行非法活动，在法律授权下政府机构的监听权也应得到保证[9]。

为取得相互间的互操作性，不同 PKI 系统需要采用一致的标准。现在 PKI 方面的标准主要包括如下三部分：

1)国际电信联盟电信部分(ITU-T)所制定的标准：X.208，X.209，X.500，X.509，X.680，X.690，等等。

2)IETF 的 PKIX 工作组所制定的标准：主要表现形式为系列 PKIX 草案和 RFC 标准，主要涉及内容有：X.509证书和 CRL 规范，证书策略和 CPS，CMP/CRS/CMC/ SCVP/DPV/ DPD/TSP/ LDAP/OCSP/DVCS，属性证书，PKIXALGS 等等。

3)RSA 信息安全公司制定的标准：公钥密码术标准(Public-Key Cryptography Standards，PKCS)系列，包括 PKCS#1，#3，#5，#6，#7，#8，#9，#10，#11，#12，#15。

一个完整的 PKI 应该至少包括以下部分[2,3]：①认证中心(CA)；②证书库(Repository)，通常为轻量级目录访问协议(Lightweight Directory Access Protocol，LDAP)服务；③证书撤消(Certificate Revocation)产生 CRL；④提供密钥备份和恢复服务的 KMC；⑤密钥更新；⑥密钥历史档案(Key History Archives)；⑦交叉认证(Cross-Certification)；⑧支持非否认；⑨时间戳服务(Timestamp Authority，TSA)；⑩客户端软件。可选的部分则包括：①注册机构(RA)；②CRL 颁发服务器(CRL Issuer)；③在线证书状态协议(Online Certificate Status Protocol，OCSP)服务器；④数字签名有效性公证服务等等。

1.3 PKI 系统的信任模型

PKI 为需要进行安全通信的双方建立了一种信任关系，使彼此间可相互信任。这种信任关系的建立都是通过对证书路径的验证来完成的。证书路径由一系列彼此按顺序相连接的证书组成，所以也被称为证书链。证书路径的起始端点被称作“信任锚”(Trust Anchor)，是验证方信任的起始点。证书路径的末端是要验证的用户证书，中间可有零个或多个子 CA 证书。

PKI 证书有效性验证方案是按照证书验证的安全策略进行[1,4]，包括：证书路径的构造或确定(若采用 PKCS#7证书链的方式则证书路径已经存在)，验证的初始化，证书有效期和各扩展项的验证，证书状态信息的获取。为确定证书状态信息，可以采用证书作废表 CRL 或在线证书状态协议 OCSP 查询两种方式。CRL 支持完整 CRL 和增量式 CRL(delta-CRL)两种方式，下载 CRL 一般采用 LDAP 协议。确定证书状态是采用 LDAP 还是 OCSP 方式由安全策略定义，一般来说，OCSP 能提供更实时的证书状态信息，适用于对实时性要求比较高的应用如电子商务等，而 LDAP 则可应用于实时性要求一般的应用如安全电子邮件等。

“信任锚”的选择和证书路径的构造方式不是唯一的，这就构成了不同的证书路径体系结构。这些体系结构包括[2,3]：

层次式(Hierarchical)：CA 以层次式的方式组织在一个根 CA 之下，严格层次结构可以描绘为一棵倒置的树。在一个层次式 PKI 中，每个服务依赖方都知道根 CA 的公钥，通过验证从根 CA 开始的证书路径来验证任何证书。根 CA 是信任的根，或“信任锚”。

网状(Mesh)：独立的 CA 通过互相交叉认证，形成对等 CA 间信任关系的一般网状拓扑结构。终端实体通常都选取直接给自己颁发证书的 CA 为“信任锚”，CA 服务依赖方通过从可信 CA 开始的证书路径中的证书来验证证书。

信任列表(Trust-list)：每个终端实体都有多个“信任锚”供选择，每个“信任锚”都是自签名的根证书。证书路径的构造也非常简单，验证方只需从被验证证书开始向上追溯，直至一个自签名的根证书。若该证书在验证方的“信任锚”集合中，那么这个证书就能被认证。最典型的是应用 Web 浏览器中内置的自签名根证书列表作为信任列表。

桥接(Bridge)：所有独立的根 CA 只需要与专门进行交叉认证的桥 CA(Bridge CA，BCA)进行交叉认证即可，而不再需要像网状模型那样两两间相互交叉认证，这形成一个以 BCA 为中心的星型拓扑结构。通过 BCA 可以将网状模型的 $(N-1)*N/2$次交叉认证减少为 N。BCA 体系结构简化了存储和管理，在不同信任域之间架起相互信任沟通的桥梁。

混合(Hybrid)：将层次式和网状或桥接两种体系结构相结合，即某些信任域内组建层次式 PKI 系统，而不同信任域之间通过根 CA 间交叉认证或和 BCA 交叉认证建立信任关系。

另外还有一种以用户为中心的信任。在一般被称作以用户为中心的信任模型中，每个用户都对决定信赖哪个证书和拒绝哪个证书直接完全地负责。尽管最初的可信密钥集合通常包括一个特定用户、个人认识的朋友、家人或同事的密钥，但这个决定可以被许多因素所影响。

层次式适用于有严格上下级关系的组织，网状或者桥接结构适用于不同的组织机构间，采用网状或者桥接模式完全取决于各 PKI 的安全策略规定和国家的宏观政策指导。

1.4 PKI 客户端的安全技术

代码签名是指对安全组件软件代码采用数字签名的技术，可以有效防范安全组件软件代码被篡改或替代，使用户免遭病毒与黑客程序的侵扰，同时可以保护软件开发商的版权利益。在每次运行安全组件之前先验证其代码签名的正确性，可以保障 PKI 客户端软件的完整性。

PKI 客户端安全设计还包括：①采用安全的密钥管理和证书管理。可采用硬件安全模块(Hardware Secure Module，

理中有一个或几个托管代理不愿合作或无法合作时，监听机构仍能很容易地重构出会话密钥。此外，该方案还具有抵抗LEAF Feedback攻击的特性。

3.2 时间戳技术

支持防否认服务的一个关键因素就是在PKI中使用安全时间戳。原来的数字签名方案虽然能确认某个数字签名与公钥证书中实体的私钥之间的联系，但数字签名产生者仍然可以在事后抵赖：该数字签名是在证书作废之后由其他人伪造产生的，根本就不是他/她产生的，所以也就不该由他/她来为该数字签名负责。时间戳服务的引入，有效地解决了该问题。

时间戳服务器以C/S模式提供时间戳服务[10]，它根据客户端所发出的时间戳服务请求，根据请求中的单向散列值产生时间戳令牌(Time-stamp Token)，这里请求中的单向散列值用客户端的私钥加密就是文档的数字签名。时间戳和数字签名都是只针对某一特定的文档。

PKI中必须存在用户可信任的权威时间源，就是能被PKI用户验证证书的安全时间戳服务器。在很多环境中，支持防否认服务是时间戳的主要目的，时间戳服务构成PKI扩展服务的一个组成部分。对时间戳服务的一些需求如下：①引进安全可靠的时间源代替目前的本地系统时间，可供选择的可信设备有全球卫星定时系统、原子钟等；②对时间戳策略的支持，包括时间戳安全策略、发布、使用和验证等；③多时间戳密钥对的支持，能对一个时间戳请求颁发一到多个时间戳令牌；④支持对成功回复的时间戳请求和时间戳令牌的备份、归档和恢复。PKI数字签名有效性公证服务(Notarization)需要用到备份时间戳令牌。

3.3 数据验证功能增强技术

数据验证包括数字签名有效性验证，而数字签名有效性验证又必然包括数字证书的有效性验证。对数字证书的有效性验证是个递归的过程。可以采用如下两种方式：(1)客户端自己验证[1,4]；(2)将证书或数据验证交给可信第三方(TTP)验证，这主要包括数据验证和认证服务器(Data Validation and Certification Server，DVCS)服务以及OCSP新提供的委托证书路径验证(Delegated Path Validation，DPV)。这些都是为满足特定的应用需求，提高PKI客户端透明性而新增的服务。

DVCS是能被用作组建防否认服务的组件的可信第三方。它目前定义四类服务[11]：①拥有数据的证实；②对拥有数据声称的证实(也就是时间戳服务)；③数字签名文档的有效性验证；④公钥证书的有效性验证。DVCS的验证结果是产生一个数据验证证书(Data Validation Certificate，DVC)。

OCSP第一版仅设计为提供在线证书状态查询服务，和支持OCSP请求的重定向。最新的OCSP规范中提供DPV和委托证书路径发现(Delegated Path Discovery，DPD)服务[12]。

DPV允许一个可信服务器执行一个验证时间T的实时证书验证，这里T可以是当前时间或一个相对很近的时间。DPV还允许在一个企业组织内以一种一致的方式来依照管理所定义的验证策略来验证，客户端能依照一个特殊的验证策略来指示服务器执行路径验证。

DPD提供这样一些优点：①以发送给一个服务器的一个简单查询取代多个证书库查询，并且服务器的缓存可降低等待时间；②对客户端系统的另一个益处是它不需要合并不同集合的软件来与不同形式的证书库交互(可能通过不同的协议，或者执行必需的图形处理来发现证书路径，分开地获取路径验证数据的查询)，只要集成进DPD的客户端软件即可。

3.4 用户漫游技术

用户漫游的目标是无论用户在何时何地，使用何种设备，只要他/她能够连接到Internet上，都能够获取自己的证明(指可被用来证实一个实体的身份，或帮助实体安全通信的信息)，从而实现用户证明的可移动性(Credential Mobility)和可移植性(Credential Portability)。用户证明包括诸如私钥、可信根CA证书、票据，或个人安全环境(PSE)的私密部分等信息。

目前强的PKI系统比较安全，但存在如下问题：①要求防篡改的智能IC卡或电子钥匙才可有效保障私钥的安全和私钥运算的安全；②不方便性：PKI经常需要用户操作交互；③在过去十年PKI部署使用的受挫经验，说明PKI并不方便使用。当在其他机器上需要使用PKI服务，但其他机器上却没有相关的驱动程序或智能IC卡读卡器时，用户将不再能正确获取PKI所提供的服务。对普通用户来说，最熟悉、最方便的验证方式是密码口令。但弱的密码系统如传统的口令验证虽说相对便于使用和可操作，但是很不安全：①容易遭受密码猜测攻击(或密码字典式攻击)；②管理员帐户有权访问客户数据。

强密码系统和弱密码系统两者之间的不同导致实现中的障碍，结果产生很多脆弱的3A(授权、鉴别和审计)系统，及很少的强PKI系统。可行的PKI策略是沿着阶段变迁的路径[13]：从脆弱的密码系统→PKI加强的密码(用户不需要改变，颁发者也不需要改变，消除了脆弱性)→带有密码方便的PKI(密码可用性，PKI的安全性)→强PKI系统。这样可以将PKI有效集成，而不是处于孤立的位置。这样做还使得用户漫游(User Roaming)成为可能。

标准RSA算法密钥对由公钥和私钥组成，它的产生过程如下：

1)产生两个大素数 p 和 q；

2)计算 $n=p*q$；

3)计算 $\lambda(n)=LCM(p-1,q-1)$，选择公共指数 e，使得 e 满足是一个在3和 n 之间的正整数，并且 $GCD(e,\lambda(n))=1$(其中 $GCD(.,.)$ 计算两个非负整数的最大公约数；$LCM(.,.)$ 计算两个非负整数的最小公倍数)。这样就得到公钥 (n,e)；

4)计算私有指数 d，使得 d 是一个小于 n 的正整数并满足 $e*d\equiv1(\mathrm{mod}\ \lambda(n))$。这样就得到私钥 (n,d)；

5)安全销毁 p 和 q。

文[13,14]提出一种已申请专利的密钥分割方法，将RSA的私钥分割成两个部分，而同样能取得标准RSA算法的功能。分割过程为：第1至第4步如上，附加如下步骤：

5)让用户选择一个密码Pwd，该密码满足密码选择规则(如长度、不同字符等要求)；

6)按照基于口令的密钥生成函数(PKCS#5)标准来产生对称密钥算法加密密钥：选择一个正整数的循环记数IC(推荐至少为1000，以增加攻击难度)，重复如下步骤：

a)选择一个随机数作为Salt；

b)计算 $d_1=PBKDF(Pwd,Salt,IC)$；

直到 $GCD(d_1,\lambda(n))=1$，并且满足 d_1 是一个小于 n 的正整数。用户保存 IC 值和最终的 $Salt$ 值。

7)计算 d_2，使得 d_2 满足：$d_1*d_2\equiv d(\mathrm{mod}\ \lambda(n))$；

8)安全销毁 p，q 和 d。这样，公钥就是 (n,e)，用户的私钥

指数是 d_1(用户知道计算得到 d_1 所需的密码 Pwd),应用程序对该用户的私钥指数是 d_2。

如果指定(n,e)为密钥 K_1,(n,d_1),为密钥 K_2,(n,d_2)为密钥 K_3,那么用密钥 K_2和密钥 K_3依次(或先用 K_3再用 K_2)对消息 M 产生数字签名可得到:

$$(M^{d_1} \bmod n)^{d_2} \bmod n = M^{(d_1 \cdot d_2)} \bmod n$$
$$= M^{(d+L\cdot\lambda(n))} \bmod n = (M^d \bmod n) * (M^{\lambda(n)} \bmod n)^L$$
$$= (M^d \bmod n) * 1^L = M^d \bmod n$$

其中 L 是个正整数。

这结果等效于直接使用原来的私钥(n,d)进行签名。数学证明,对攻击者来说,分割后的3密钥 RSA 系统和原先的2密钥 RSA 系统同样安全,相关安全性分析证明见文[14]。

3密钥 RSA 模型中密钥 K_1将被包含在 X.509数字证书中;密钥 K_2可以根据用户输入的口令得到。在将来,可以存放在用户的智能卡中,或从用户的生理特征或结合多种因素得到;密钥 K_3则通过合作签名者如安全身份设备保存,如图3中所示。最终得到的用户使用框架为实用的 PKI 由传统的 PKI 和密码组合而成,它可与一般的 PKI 标准同样使用并可互操作,并支持用户的漫游。

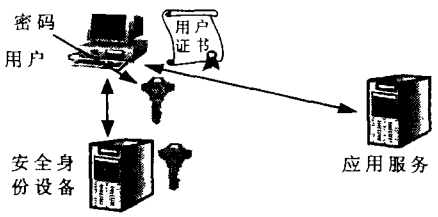

图3 密钥分割实现3密钥示意图

为支持用户漫游,文[15,16]描述 SACRED 方案的需求和框架模型,提出至少有两种可行的提供用户证明可移植性的解决方案。第一种解决方案涉及使用"证明服务器",用户可以从一个设备中把证明上载(Upload)到证明服务器,通过帐户管理把证明保存在证书服务器,在任何需要的时候可以被用户指定的设备下载(Download)和使用。当然,在上载和下载的过程中需要用到单向或双向身份认证,支持基于公钥密码体制的认证和基于口令的强身份认证(如 RFC 2945中介绍的 The SRP Authentication and Key Exchange System, Secure Remote Password)。第二种解决方案涉及从一个设备到另一个设备的证明"直接"传输(如从一个手机到一个 PDA)。该过程中即使有其他服务器参与,它们也没有积极协助安全交换。

前面3密钥 RSA 思想完全可以和后面的 SACRED 结合起来,并取得很好的实际应用价值。

3.5 支持 WPKI 及与有线网络的互操作技术

现在的 E-commerce 今后将会有很大部分由移动商务(Mobile-commerce,M-commerce)来完成。鉴于移动设备存储容量小、运算能力低等特点,在部署证书应用时必须考虑这些特点,但安全性不能降低。由 WAP 论坛(WAP forum)提出的改进主要包括[17]:①限制证书的大小;②限制证书最大路径长度为3;③限制证书序列号最大为8字节;④限制采用的签名算法为 sha1WithRSAEncryption 和 ecdsa-with-SHA1。采用 ECDSA 不仅可以使证书中包含的公钥长度显著变小,而且取得同样安全等级所需的运算能力也较小;⑤对一些证书扩展项的限制。

由于无线通信采用 WAP 协议,而在 Internet 中广泛采用的则是 TCP/IP 协议,两者相应的传输层安全协议则分别为 WTLS 和 TLS。为使无线设备能够访问 Internet 中的商务网站,必须解决它们间的互操作性问题。这主要通过一个嵌入在 WAP 网关中的 WAP 连接器来实现,WAP 连接器为无线通讯用户提供专用的 WAP 证书服务。WAP 连接器位于 CA 认证中心与 WTLS 网关之间,起到一个桥梁的作用,可以无缝实现无线用户和网络用户之间的端到端安全性。组织结构如图4所示。

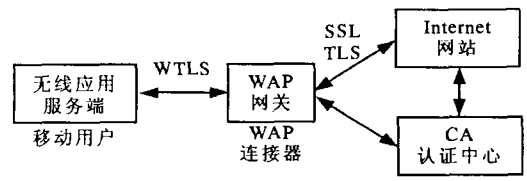

图4 WPKI 结构示意图

3.6 对授权管理基础设施的支持

Privilege Management Infrastructure (PMI),即特权管理基础设施或授权管理基础设施,是属性证书、属性中心、属性证书库等部件的集合体[4]。基于 PKI 的公钥身份证书,认证中心 CA 身份认证系统和基于 PMI 的授权系统间相互协作,而 PMI 可以看成是 PKI 体系的扩展。业务应用系统可通过 PMI 来实施授权策略,即:对不同用户、不同的信息设置不同的访问权限。PMI 特别适合基于角色的访问控制(Role-Based Access Control,RBAC),在属性证书中的属性可以包括用户的属性、组或角色等信息[4,18]。

将公钥身份证书和属性证书绑定可有不同方法,特别有整体式、自治式的和连锁式签名三种方式[19]:(1)整体式签名是指身份证书和属性证书信息绑定在单独一张公钥证书中,而包含序列号,颁发者,有效期等的信息则能被共享。这通过使用 X.509 V3证书和它的主体目录属性(Subject Directory Attributes)扩展项很容易实现;(2)自治式签名支持多个 CA 和身份及属性证书的不同使用期限,身份和属性间是一种松偶合绑定机制;(3)连锁式签名像自制式签名一样支持多个 CA 和身份及属性的不同的使用期限,但它提供一种在身份和属性间的紧偶合绑定机制。使用某张具体公钥身份证书的数字签名代替真正的身份信息,换句话说,一张属性证书必须引用一张具体的公钥身份证书,该证书的数字签名和属性证书相结合。

4. PKI 系统总体技术探讨

4.1 可扩展性的提高

PKI 系统三大提供商 Entrust、VeriSign 和 Baltimore 之一的 Baltimore 公司提出可扩展性一种方案,他们称之为"克隆"的技术。在当前的服务器群性能满足不了应用需求时,可以将服务器克隆一份并加入到原服务器群,利用分布式系统和负载均衡技术对外提供服务。而对于服务器中的签名密钥对和其他密钥对,在克隆过程中,利用硬件安全模块(HSM)的备份恢复功能,多备份一份 HSM,这样备份的硬件安全模块将拥有与 HSM 完全相同的密钥对。克隆技术的最大优点是整个系统结构变动极小,不要改变整个 PKI 系统的体系结构,而只需要考虑加入新服务器后的服务器间的负载均衡问题。

提高可扩展性的另一种方法是对服务器的HSM重新创建新的签名密钥对和加密密钥对等，利用X.509 V3规范所提供的Authority Key证书扩展项[1,4]来指定不同CA签发服务器的不同签名密钥对，再建立分布式的系统对外提供服务。

另外，对于需要向用户提供在线服务的RA服务器、LDAP服务器、OCSP服务器、KMC服务器等，都可以按照分布式方式部署，在需要的时候提高原服务器的性能或增添新的服务器，并完成任务调度和负载均衡等工作。特别地，LDAP服务器和OCSP服务器都支持查询的重定向功能，能够以类似于DNS服务器的方式部署层次式的服务体系，LDAP还可以实现类似于分布式数据库的分布存储。

4.2 互操作性的提高

解决多个PKI厂商之间的互操作性是PKI论坛(PKI forum)在2001年的几个主要目标之一。被PKI论坛所采用的PKI互操作性可以识别为三个层次的互操作性领域[20]。分别为：

1)组件层(Component-Level)互操作性包括：①必须实现在可适用的PKI组件间(如CA、RA及终端实体EE)的通用协议，消息格式和证书格式；②必须实现PKI组件间的实体验证和数据交换保护的通用算法；③必须支持一种存储库和PKI组件间证书和证书状态信息的方法；④不管是以何种方式存储的，经授权的终端实体必须能够安全地访问私钥；⑤必须支持一到多种证书状态机制。

2)应用层(Application-Level)互操作性包括：①证书和证书状态信息必须兼容；②为确保证书按照预定的密钥用途和在任何相关的限制下使用，必须实现业务控制；③算法必须兼容；④数据封装和编码格式必须兼容；⑤对等实体间交换信息的底层通信协议必须兼容；⑥任何以带内方式共享的、与公钥相关的信息必须兼容。

3)域之间(Inter-Domain)互操作性：这包括技术的和策略相关的内容。①需要有建立PKI域之间信任关系的方法；②适当的PKI相关信息必须在PKI域之间相互可以获取；③每个PKI域必须同意遵循某些安全策略，并且每个PKI域需要有适当的机制来确保实施所同意的安全策略。

4.3 透明性的提高

PKI透明性的提高主要体现在PKI需要用户干预的情况变少，只要用户在第一次注册时完成身份认证并获取HSM。透明性的提高主要得益于PKI在线服务功能的支持。

PKI透明性的具体表现有：①选择是否需要备份加密密钥对后，将自动向密钥管理中心请求加密密钥对，并安全下载安装到本地HSM中；②自动请求加密证书并将证书下载到本地HSM中；③所有证书和密钥对的到期自动更新管理；④数字签名验证工作的自动透明完成；⑤恢复数据加密密钥对和密钥历史档案检索的透明完成，加密数据的自动恢复等。用户无需知道所有这些实现的细节和运作流程，可以认为这些对于用户来说都是透明的。PKI的总体需求是用户能够透明地获得安全基础设施(PKI)所提供的安全服务。

但有些情况还是需要用户交互，这样的操作包括数字证书的作废、挂起和挂起恢复，或HSM设备的损坏更换。这主要是因为仅仅依靠程序软件无法判断密钥对是否泄密或被盗，或者在什么时候需要暂停数字证书和密钥对的使用，而什么时候又能恢复正常使用。

4.4 第二代PKI技术

对于第一代PKI来说，PKI所支持的应用产品中需要包括证书用户的密钥管理功能和证书管理功能，和集成在应用中的PKI功能，相互间的协议都是基于ASN.1语法。因此，第一代PKI将很难实现应用层的透明性。

可扩展标记语言(Extensible Markup Language，XML)作为一种数据格式具有明显优势，在Web系统中采用XML数据格式，将极大地增加系统的灵活性、互操作性和扩展性。能用于Web Services中的XML已有信任服务标准有[21]：XML签名(XML-DSIG)、XML加密(XML-ENC)、XML密钥管理规范(XML Key Management Specification，XKMS)、XMKS大量注册操作(XML KeyManagement Specification Bulk Operation，X-BULK)、安全声明标记语言(Security Assertion Markup Language，SAML)等。

XKMS由两部分组成[21,23]：XML密钥信息服务规范(XML Key Information Service Specification，X-KISS)和XML密钥注册服务规范(XML Key Registration Service Specification，X-KRSS)。PKI与XML相结合形成第二代PKI以提供信任服务[22]，如图5所示。

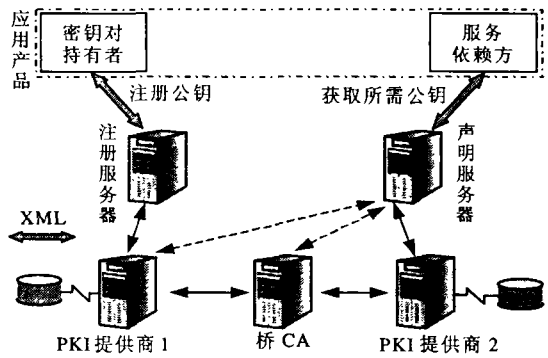

图5 XKMS结构示意图

X-KISS定义一个支持应用授权给服务来处理与XML签名、XML加密和其他公钥等密钥信息的协议，功能包括所需密钥的定位和描述密钥到身份信息的绑定。X-KRSS定义一个由密钥对持有者注册密钥对的协议，注册的密钥对以后可用在X-KISS或诸如信任声明服务规范(Trust Assertion Service Specification，XTASS)等高层信任声明服务中。X-BULK则是在X-KRSS的基础上对XKMS的扩展，但它不是X-KRSS的一个接一个的注册，而是采用大批量的注册，同时可以支持一些已经盛行的规范标准如采用智能IC卡、PKCS#10标准的注册请求、PKCS#1标准的密钥对等等。

采用XKMS规范，可以支持XML应用的安全需求，并减少部署PKI的障碍，主要表现在：①支持能力受限的移动设备；②实现应用层的PKI透明性：将复杂性从客户端移到提供可信XKMS服务的服务器上，客户端只需支持XML和基本的密码功能，而不再需要合并复杂的PKI功能。

5. 存在的风险和问题

5.1 PKI系统存在的风险

PKI虽然在理论研究和实际应用中都取得了很大进展，但PKI仍存在如下风险[24]：

①我们信任谁，为何信任：一个CA常常定义为可"信任"的，但CA其实只是保证公钥和实体名称信息的组合是可信的，而并不保证那个实体对其他用户来说是可信的；②谁在使用我的密钥：针对CA系统的一个最大风险是怎么保护自己的私钥。一个普通用户几乎不可能拥有一个安全的计算机系

统，从而无法确保私钥的存储和使用安全；③验证计算机的安全性：攻击者如果能够增加他自己的公钥证书到可信证书列表中，然后他就能发布他自己的证书，而这些证书会被当作合法的证书而得到信任。唯一的解决方案是所有证书都在一台无懈可击的可信计算机上校验，且它能经受得住各种渗透测试和物理攻击；④难以确定某个具体用户：X.509要求以一种全局唯一的名称来标识用户，但用户可能存在同名现象，导致使用过程中很难仅根据证书中的身份信息区分究竟哪个才是自己想要的；⑤CA是否是授权中心：有些公钥证书同时拥有访问控制权利，但CA一般只能证明用户的身份信息，而不是权威中心，CA通常没有授权的权利。这将导致公钥证书使用在访问控制中的矛盾；⑥用户是否为安全设计的一部分：PKI安全设计时很难真正把用户看作一部分；⑦采用单CA还是CA+RA模式：为确保安全性，采用一个CA更安全；但为确保可用性，需要采用CA+RA模式，但这会带来更多安全威胁；⑧CA如何鉴别证书的拥有者：CA在颁发证书之前都需要识别证书的申请者，CA以何种方式来识别申请者，以及如何验证申请者确实控制着与被验证的公钥相对应的私钥；⑨证书操作是否安全：如果想使系统安全的话，证书必须正确地使用；⑩为何我们仍在使用CA过程：基于数字证书的单点登录(SingleSignOn，SSO)身份验证方式提高了系统安全性，身份认证过程符合PKI/X.509强身份认证协议。但认证的安全价值都被单点登录机制完全破坏，如果用户离开计算机一会儿，任何经过该计算机的人都可以在单点登录机制的环境下进行一些非法签名或其他什么操作，或者病毒、木马等也可能进行一些非法签名。

5.2 PKI-CA机制其他的不足

1)缺乏对匿名性的支持：在某些特殊应用场合下，如匿名电子现金或匿名选举等，数字签名就显得无能为力。

2)对私人信息的保护和共享仍然是空白：私人信息以静态的明文状态在数字身份证书中提供，既没有隐私保护功能，也没有很好的共享特性。

3)缺乏“电子公章”的支持：“电子公章”在应用密码学中被称为“团体签名”技术。目前PKI并不能实现技术意义上的“团体签名”。

结束语 PKI技术取得了很多进展，但仍然存在一些问题有待研究解决。PKI如何保证对将来Web Services和新出现应用支持的同时，仍保持对目前一系列已经支持应用的支持，是将来需要解决的问题。另外，PKI和其他的安全信任机制如PGP、SPKI等之间能否相互协作，以共同实现安全基础设施的目标，都有待研究和探讨。

参考文献

1 Housley R, Polk W, Ford W, Solo D. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280, Apr. 2002

2 Advances and Remaining Challenges to Adoption of PKI Technology, U.S. General Accounting Office. Feb. 2001

3 Burr W E. Public Key Infrastructure (PKI) Technical Specifications: Part A-Technical Concept of Operations: [WORKING Draft]. Federal PKI Technical Working Group. Sep. 1998

4 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. ISO/IEC 9594-8, Aug. 2001

5 Marchesini J, Smith S W. Virtual Hierarchies: An Architecture for Building and Maintaining Efficient and Resilient Trust Chains: [tech. rep.]. TR2002-416, Depart. of CS, Dartmouth College. Feb. 2002

6 荆继武，冯登国. 一种入侵容忍的CA方案. 软件学报，13(8)：1417～1422

7 Levi A, Caglayan M U. An Efficient, Dynamic and Trust Preserving Public Key Infrastructure. In: IEEE Symposium on Security and Privacy (S&P 2000), Berkeley, California, U.S. May 2000

8 Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management. In: IEEE Symposium on Security and Privacy, Oakland, Ca, U.S. May 1996

9 曹珍富，李继国. 基于ElGamal体制的门限密钥托管方案. 计算机学报，25(4)：346～350

10 Adams C, Cain P, Pinkas D, Zuccherato R. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). RFC 3161, Aug. 2001

11 Adams C, Sylvester P, Zolotarev M, Zuccherato R. Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols. RFC 3029, Feb. 2001

12 Pinkas D, Housley R. Delegated Path Validation and Delegated Path Discovery Protocol Requirements. RFC 3379, Sep. 2002

13 Sandhu R. Role-Based Access Control with SingleSignOn. Net's Practical PKI Appliance. In: 17th Annual Computer Security Applications Conf. (ACSAC'01). New Orleans, Louisiana, U.S. Dec. 2001

14 Bellare M, Sandhu R. The Security of Practical Two-Party RSA Signature Schemes. http://www.cse.ucsd.edu/users/mihir/papers/splitkey.html, 2001

15 Arsenault A, Farrell S. Securely Available Credentials - Requirements. RFC 3157, Aug. 2001

16 Gustafson D, Just M, Nystrom M. Securely Available Credentials - Credential Server Framework. http://www.ietf.org/internet-drafts/draft-ietf-sacred-framework-05.txt. Sep. 2002

17 WAP Certificate and CRL Profiles WAP-211-WAPCert. http://www.wapforum.org. May 2001

18 Farrell S, Housley R. An Internet Attribute Certificate Profile for Authorization. RFC 3281, Apr. 2002

19 Park J S, Sandhu R. Binding Identities and Attributes Using Digitally Signed Certificates. In: 16th Annual Computer Security Applications Conf. (ACSAC'00). New Orleans, Louisiana, U.S. Dec. 2000

20 Brink D, et al. PKI Interoperability Framework: [White Paper]. PKI forum Technology Working Group. Mar. 2001

21 Hallam-Baker P. XML Key Management Specification. XKMS seminar, Apr. 2001

22 Ford W. The Future of XML and PKI Towards Interoperable Trust Services. XKMS seminar, Apr. 2001

23 Hallam-Baker P. XML Key Management Specification (XKMS 2.0): [Working Draft]. W3C. http://www.w3.org/TR/xkms2/. Mar. 2002

24 Ellison C, Schneier B. Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure. Computer Security Journal, 2000, 16(1)