专著 出版基金资助项目 ZIZHU XIANGMU

ZHUANZHU

信息安全体系架构及相关技术

张丽娜 著

ZHUANZHU

西北工业大学出版社

信息安全体系架构及相关技术

张丽娜　著

西北工业大学出版社

【内容简介】 本书从密码学的角度全面地分析和讨论了信息安全体系架构及其相关技术。全书大致可分为四部分。第一部分概述安全体系架构的基本知识，包括安全系统概述、安全系统的构架、安全系统的结构、安全系统的工作原理。第二部分全面分析了各种密码算法，阐述了从最底层的模块到机制实现的关键技术。第三部分主要分析了安全密码芯片的相关技术，讨论了基于 SOC 的调整、通用的公钥密码芯片设计方法；在硬件上描述了芯片 SOC 结构的设计与搭建，以及良好有效的仿真和测试方法。第四部分讨论了安全相关技术问题。书后附有本书主要算法的 C 程序实现代码。

本书可作为高等学校信息安全、计算机、通信工程、密码学及相关专业大学本科生和研究生的教材，可也供从事通信工程和计算机网络工程等理论应用研究的科研人员和工程技术人员参考。

图书在版编目(CIP)数据

信息安全体系架构及相关技术/张丽娜著．—西安：西北工业大学出版社，2014.8
ISBN 978-7-5612-4065-6

Ⅰ.①信… Ⅱ.①张… Ⅲ.①信息系统—安全技术 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字(2014)第 180565 号

出版发行：西北工业大学出版社
通信地址：西安市友谊西路 127 号　　邮编：710072
电　　话：(029)88493844　88491757
网　　址：www.nwpup.com
印 刷 者：兴平市博闻印务有限公司
开　　本：787 mm×1 092 mm　1/16
印　　张：13.5
字　　数：328 千字
版　　次：2014 年 8 月第 1 版　2014 年 8 月第 1 次印刷
定　　价：39.00 元

前　言

自20世纪90年代以来，随着科学技术的高度发展，人类已经进入了信息时代，如何保证信息的安全性，解决信息的真实性、保密性、完整性和不可否认问题，成了现阶段发展的一个重要问题。信息安全是一个整体全局的观念，必须从体系架构入手来提出解决方案。因此信息安全体系架构及其相关实现技术成为了安全开发和安全应用所面临的最关键问题之一。

本书主要从密码学的角度分析和论述了信息安全体系架构及其相关技术，从系统的观念分析信息安全体系构架必须具备的要素和基本构建方法，希望提出一种思路和方法来更好地构建信息安全体系。本书希望从信息的加密保护、用户的身份认证、信息的安全交互与确认等更偏重于密码学的内容来阐述构架信息安全体系架构的核心技术，这些方面是搭建任何网络经济信任体系的基石。对于不同的安全需求，安全保护定义的程度也是不同的。在不同的安全层次，不同的密码学应用提供不同的安全保障。

本书从体系架构入手提出信息安全体系架构实现思路和结构模型，根据信息安全体系架构思路，提出并设计了信息安全体系应用模型。从清晰的层次化功能划分，到设计流程，再到整体解决方案，均给出了实际的实现方法。全面分析了包括ECC和RSA在内的各种密码算法，讨论了从最底层的模乘模块到机制实现的关键技术；在理解底层模块算法的基础上给出安全芯片的核心设计和实现方法，给出了基于SOC的调整、通用的公钥密码芯片设计方法，在算法上分析了关键核心模块的技术，以及安全密码芯片的相关技术和实现思路。此外还讨论了基于虚拟机的软件保护相关技术和网上银行安全支付相关技术。

在信息安全体系架构的实现过程中，会遇到各类问题，必须将设计与实际需求和情况相结合，才能提出符合实际的全面解决方案。由于密码实现的算法灵活、多变，因此必须根据实际情况选择最适应实现方法。此外，各类安全密码机制、数据处理的软/硬件实现算法理论和设计方面都有待进行更加深入的研究，高速度、低成本、低功耗、多功能等约束条件下的硬件模块的实现技术也有待提高。

现在我国在信息安全领域急需一套完整的系统安全解决方案，相信本书是一次有益的探索与实践，具有很强的现实意义。

笔者参加工作近几年的研究及读博期间的主要成果成为本书的主要素材。在本书的写作过程中，笔者参阅了国内外的相关著作，在此，向其作者表示诚挚的谢意。同时，对给予本书的写作、出版以帮助的老师、学者表示衷心的感谢。

感谢笔者所在单位西安科技大学计算机学院各位领导和同事的大力支持与帮助，感谢西安科技大学人事处、科技处及各相关机构各位老师给笔者学业和工作上的精心安排、指导与关心，感谢笔者读博期间的导师陈建华教授及武汉大学密码研究中心技术研究团队的所有成员。

特别感谢西安市软科学研究项目、西安科技大学博士启动基金和西安科技大学培育基金等的资助。

由于水平所限，书稿虽几经修改，仍难免存在缺点或疏漏，恳请专家、同行和广大读者批评指正。

作　者

2014 年 5 月

目　录

第1章 引 言

1.1 研究背景

自20世纪90年代以来，科学技术的高度发展已经毋庸置疑地把我们带进了信息时代，随着信息以爆炸式的速度不断在我们生活中的每一个角落涌现，如何确保信息的安全即信息安全问题成为全球关注的热点。

在过去两个世纪中，工业技术是影响军事实力和经济实力的关键，而在21世纪，信息技术将成为主导因素。随着国家经济对信息化的依赖越来越强，信息安全的地位日益凸显，它已经成为了国家安全的一个重要组成部分。各种机密信息若是在网上暴露，将会给国家带来巨大的现实威胁。目前各国政府在信息安全管理方面的定位主要就是保障网络化时代的国家安全和利益。

在国内，随着社会信息化程度的不断提高，信息技术应用领域的不断拓展和网络新技术的不断更新，网络和信息安全问题所带来的负面影响也日益突出。解决网上银行、电子商务、电子政务、网上证券、会员管理、数字机顶盒等安全问题的需求也越来越迫切，信息安全问题成为制约我国信息产业发展最基本和紧迫的问题。而信息产业的发展已经成了推动经济发展和社会进步最强有力的手段，只有走经济信息化的道路，积极主动地与国际接轨，才能在世界经济竞争中立于不败之地。因此，必须要解决好信息安全问题，为我国信息产业的大力发展和下一次革命提供有力的保障和基础。

目前大多数的信息安全防护手段都集中于比较单一的网络周边防护产品上，如病毒防护、网络防火墙、入侵检测等等，但是任何单一的安全技术和手段，都不能与计算机网络与信息系统所面对的众多安全隐患相抗衡。我们的安全观必须要从“单一信息安全产品防护”发展到“综合防御体系防护”，安全建设必须要从“某一点的安全建设”过渡到“整个安全体系的建设”。

因此系统中的安全应该是一个整体全局的观念，必须从体系架构入手来提出解决方案。这里所讲到的安全，并不是通常所提到的病毒防护、网络防火墙、入侵检测等为整个系统外围建立安全保障环境的技术手段，而是指信息的加密保护、用户的身份认证、信息的安全交互与确认等更偏重于密码学的内容，这些方面是搭建任何网络经济信任体系的基石。这些基本方面的安全功能往往是由不同的安全元件实现的，并且需要在完善的体系架构中互相配合。

1.2 对信息安全与安全观的理解

所谓的“信息安全”，是指保护信息财富，使之避免偶发的或有意的非授权泄露、修改、破坏或丧失处理能力。信息安全一般包括三重含义，即信息的机密性、真实性和完整性。

信息的机密性：是指信息没有泄漏给非法的用户，而仅仅掌握在合法的用户手中，保证合

法用户秘密拥有和使用信息的权利。

信息的真实性：是指信息没有被偶发或有意地修改、替换或伪造，保证合法用户可以拥有和使用真实的信息。

信息的完整性：是指要保证具备恢复信息错误的能力和手段，使得合法用户在任何需要的时候都能够拥有和使用正确的信息。

大家提到安全的时候，会提到很多具体的安全现状，如服务受阻、信息泄露；或者提出很多具体的信息安全产品，如防火墙、防病毒软件、VPN、安全网关、安全目录等等。但是需要指出的是，安全必须是一个系统的概念，它不仅仅指防火墙、入侵检测、漏洞扫描、网络隔离或者授权认证等等，必须全面了解整个系统存在的风险和挑战，必须从全局的、系统的观念出发，构建一个良好的安全体系架构，明确要做什么，能达到什么目的。本书从系统的观念分析安全体系构架必须具备的要素和基本构建方法，希望提出一种思路和方法来较好地构建安全体系。

对于安全的理解，业界尚存在很多争议，这也正是“安全”无法定义的原因。

通常，我们认为，如果能够抵御某种可能造成损失的攻击，那么在这个方面就是安全的。例如：使用密码算法加密消息可以抵御消息泄露所造成的损失，那么，使用了加密算法加密消息的机制在泄密方面就是安全的。所以在评估安全以前，必须了解常用的攻击方法，用攻击来评估安全。

对于不同的安全需求，安全保护定义的程度也是不同的。例如：国家机密需要非常严格的保密措施，涉及国家机密的企业则同样需要严格的保密措施，但是，如果仅仅涉及商业机密，其损失不会影响到国计民生的，需要的保密程度则低得多。同样，如果对手是国家级别的，则对手的攻击能力会强得多，需要的安全措施就强得多。如果对手仅仅是普通企业，则不需要那么强的安全保护措施。当然，国家一般不会对某个普通企业的普通商业机密有兴趣。所以在评估安全以前，必须了解对手的攻击能力，用对手的攻击能力来评估安全。

其次，安全是相对于攻破所需时间以及机密有效期而言的，只要在机密有效期之内未被攻破，则此机制是安全的。给予对手无限的能力及无限的时间，任何安全机制都可以被攻破，但这是不现实的。例如：某商业机密为某企业下季度预计发行的新产品，此机密的有效期为 3 个月，但是其竞争对手花了 1 年的时间，破解了其商业机密，那么此举是完全没有意义的。所以在评估安全以前，必须了解机密的有效期，用攻破周期和机密有效期来评估安全。

综上所述，总体安全观主要应从下述几方面理解。

(1)安全是定义在被攻破的基础上的，不能被攻破，则视为安全。

(2)不同的密级，需要的安全保护程度是不同的，安全应相对于对手的能力而言。

(3)安全是有一定有效期的，有效期内不能被攻破，则视为安全。

(4)在安全方面，主要使用密码学。在不同的安全层次，不同的密码学应用提供不同的安全保障。

1.3 我国信息安全现状

目前我国在信息安全领域急需一套完整的系统安全解决方案。首先是设计和实现安全密

码算法，包括对称密码算法、非对称密码算法、数据压缩算法和随机数生成算法。其次在此基础上研究高强度、高性能和标准化的密码专用芯片和产业化的低端智能安全芯片。再次，使用芯片替换现有安全协议中的密码算法，实现真正可信的安全协议。最后，综合各类协议，搭建一套安全系统，使得各种应用能够在完善的安全系统中运行。

密码算法是安全系统的核心和基础。密码算法的安全性，直接影响到整个安全系统的安全性，国际上已经有一系列的密码算法标准，一些密码算法标准也有充分的理论根据和广泛的评测。然而某些密码算法标准，由于制定者的原因，没有公开标准中的某些细节，虽然根据使用环境和使用对象的区别，可以直接应用这些密码算法，但是，在某些特殊场合，或某些特殊的应用中，就必须采用完全信任的密码算法。因此，密码算法的研究和制定，是我国信息安全领域中需要重点关注的。

信息安全芯片的研制水平代表着一个国家信息安全的水平，信息安全产业现已成为信息产业中发展最快、市场前景最广的高新技术产业。随着电子身份证、银行IC卡、市民一卡通等信息安全类集成电路产品在国内得到进一步推广和普及，安全芯片和安全IP核的设计和研究已经成为刻不容缓的事情。

随着社会信息化程度的不断提高，信息技术应用领域的不断拓展，网络新技术的不断更新，越来越多的应用采用了安全协议，无论是网络信息传输，还是信息管理，安全协议的安全应用和实施同样重要。由于协议的安全性可以得到形式化的证明，因此，协议的安全性不能靠经验和安全运行时间的延迟来保证，对于各种安全协议，都需要完整的形式化证明。而对于协议所使用的密码算法，一定需要可靠的实现以及正确的部署。因此，研究协议层的安全，同样具有重要的意义。

安全是不断增长的社会需求，是相对的而不是绝对的，也是动态的和不断发展的。安全观也是一个持续发展、不断完善的过程。

1.4 本书研究目的和写作规划

希望通过分析安全系统的架构和发展现状，提出合理的体系结构层次划分，从安全系统架构、安全算法、专用芯片以及安全协议等几个层次来建立安全观和构架安全系统。

本书主要包括引言、安全体系架构的分析和设计、密码学概述、数学基础、安全算法与密码技术的分析与设计、椭圆曲线安全芯片分析与设计、安全协议的分析与实现、其他相关安全技术研究等若干部分。

安全体系架构，主要论述目前主流的安全系统解决方案(PKI,CORBA,SOA)，包括安全系统概述、安全系统的构架、安全系统的结构、安全系统的工作原理，并提出了自主设计的安全系统模型和有效解决方案，论证了本体系架构的有效性、可实施性、高效性。

数学基础，主要论述本技术涉及的基本数学基础，包括群、环、域、模运算和同余等的基本概念，欧拉函数与欧拉定理，辗转相除法及中国剩余定理等。

算法设计，全面分析了包括ECC和RSA在内的各种密码算法，阐述了从最底层的模乘模块到机制实现的关键技术。比如ECC从底层模块模乘运算，到点加点倍运算，再到点乘运算

的实现，RSA 中关键技术素数生成，等等。

安全芯片设计，主要分析安全的密码芯片的相关技术，介绍了基于 SOC 的高速、通用的公钥密码芯片设计方法；在硬件上描述了芯片 SOC 结构的设计与搭建。从芯片结构开始，分析了安全芯片的抗侧信道结构设计、密钥管理、芯片仿真和测试方法。

现在我国在信息安全领域急需一套完整的系统安全解决方案，相信本书是一次有益的探索与实践，具有很强的现实意义。

第2章　信息安全体系结构的分析与设计

2.1　信息安全体系架构研究现状

信息安全体系架构是安全开发和安全应用所面临的最关键问题之一，它决定了各种安全应用如何在信息系统中组织起来，为系统提供一个整体的安全解决方案。10年前，信息安全体系通常采用“自上而下”的构建流程；由于实现的安全功能特定且单一，因此自上而下的设计模式在一定程度上满足了当时的设计和实现需求。但是从Internet的发展现状和安全需求出发，现在需要先“自下而上”，然后再从全局规划，从实现的功能和层次上实行“上下结合”，构成安全体系。安全体系不能做到一劳永逸，是在动态中求发展的。需要用发展的眼光构建和设计安全模型。

信息安全体系架构从安全概念的产生、安全模型的建立、安全体系产品的发展、安全策略的制定和实施等很多方面，经过数10年不断发展和完善，有了较多新进展和新突破。

信息安全体系中两个基本概念就是身份认证和访问控制权限，因此身份识别成为信息安全体系中最基本也是最重要的技术之一。20世纪80年代，为了解决身份识别问题中最关键的密钥管理问题，产生了PKI(Public Key Infrastructure，公钥基础设施)的概念，随后的10年中，各种围绕PKI的组织、论坛、解决方案、实现标准应运而生。PKI的发展为电子商务、电子政务及其他各类网络业务的发展奠定了坚实的基础，起到了十分重要的作用。经过多年的发展，PKI体系由于具有稳定、解决方案成熟等显著优点，使得基于PKI的安全体系架构成为目前最有效且应用最多的解决方案之一，其中的私钥分发也有了更多的表现形式，有可在计算机中保存的软件证书，也有存在于硬件中的UKEY证书、IC卡证书等等。

随着PKI体系的发展和身份认证问题的解决，在此基础上的各类安全系统结构和应用也得到了很好的发展。到现阶段为止，大部分的安全服务功能也都是基于PKI体系的。大家都知道，不论是软件还是硬件，良好的通用接口是模块复用、提高效率、节约成本的关键，各种标准制定组织也定义了很多的协议、接口来实现统一规范。

在PKI之上最典型最直接的一个应用就是API(Application Programming Interfaces，应用编程接口)，它根据PKI体系总的协议，规定通用接口，为上一级提供PKI服务。目前API没有统一的国际标准，大部分都是操作系统或某一公司产品的扩展，并在其产品应用的框架内提供PKI服务。其中以IETF建议标准的GSS－API(Generic Security Service Application Program Interface，通用安全服务应用编程接口)为代表，它提供了一种接口与网络机制和网络协议相互独立的实现。2002年，Intel提出了CDSA的结构，实际上也可以看作是在PKI基础上发展起来的一种安全通用接口。

近几年迅速发展的中间件技术使得信息安全体系结构有了新的思路，并使其成为构建信息安全体系架构不可缺少的关键技术。从传统中间件到现在的基于CORBA(Common Object Request Broker Architecture，公共对象请求代理体系结构)的中间件、3层结构、构件、

Web 服务等等，其中风头最劲的当属 SOA(Service Oriented Architecture，面向服务的架构)。这些新提出的技术实现方法为我们提供了很多新的思路。

PKI 是以分散的方式来建立密钥体系，由根 CA 为信任根，以多级 CA 来建立信任链。随着 PKI 体系的不断发展和应用，也出现了很多急需解决的问题，如可信的第三方扮演了过于重要的角色，各国以及国家各系统都各自建立了 CA 系统，CA 系统之间的相互认证和可信度成了需要解决的繁重问题。

因此一些新的系统架构开始被探索和发展。

如 IBE(Identity Based)，它以集中的方式管理密钥，TA 为信任根。Shamir 在 1984 年最早提出基于身份加密(IBE)概念，以标识直接与公钥绑定，其初衷是简化电子邮件系统中的证书管理。由 D. Boneh 和 M. Franklin 于 2001 年设计出了基于身份的实用加密方案(IBE)，直接把标识当公钥，不需要第三方认证，从而取消了 CA 机构，适用于从属关系明确的认证。但需要集中管理标识特征库，产生对应的私钥并分发，还需要在线动态管理，系统还是比较复杂。正如 Shamir 所指出的，基于身份的加密方案天生就是密钥托管的；可信第三方知道所有用户的私钥，并且密钥的分发和管理仍然是一个大问题。

又如 TM(Trusted Module)，对可信计算平台的研究主要针对目前计算机面临的各种病毒代码、木马程序以及互联网中各个节点的身份验证、信息传输等迫切期望解决的难题。可信计算平台有 4 个主要功能：身份可识别认证、平台系统环境配置的正确性、应用程序的完整性和可基于网络的验证。可信计算平台中最核心的内容就是 TPM(Trusted Platform Module)，TPM 是一个含有密码运算部件和存储部件的 SOC 芯片，它以各种形式嵌入到系统的主板上，通过合适的总线结构与主板上其他资源进行数据交换。TPM 和系统主板是以物理形式结合的，在系统使用过程中不可能被拆开。可信计算平台就是以 TPM 为核心安全模块构建可信的计算机系统，进行用户身份识别、信任链的创建和控制软件运行的可信。可信计算平台监管计算机范围内的资源，可信计算平台的软件、硬件都由 TPM 安全芯片作可信认证。

综上所述，目前信息安全体系结构的研究经历了下述几个阶段。

Entrust 公司的 Entrust/PKI 结构，现在已经成为事实上的工业标准。

IETF 提供了通用安全服务应用编程接口 GSSAPI(RFC2078)标准。

Intel 在 2002 年提出了 CDSA 的结构。

Sun 公司提出了 JASE JAVA 结构，明确了组件级应用的安全发展方向，这个标准框架也成为电子商务事实标准。

在国内，基于中间件体系架构的市场日趋成熟，但是大都集中于传统的消息中间件和交易中间件。

在 2004 年左右新一代的体系结构一般是基于 CORBA 规范的对象中间件和基于 J2EE 的应用服务器。

在 2006 年，开始了基于 SOA(Service Oriented Architecture)，建立面向服务的架构，它和 J2EE 技术一起，用客户端/服务器的设计方法。

本章从基础 PKI 体系开始，详细分析 PKI 体系的结构特征和发展思路，再介绍在此基础上产生和发展的中间件技术和可信平台体系架构。最后在分析和总结上述体系结构的基础上，提出自主创新的信息安全体系架构实现思路和构建方法，及按照此种方法架构的典型安全应用和安全系统。

2.2　基础 PKI 体系介绍

2.2.1　基于 PKI 的体系结构

全球经济发展进入了信息经济时代，网络给世界经济带来了巨大的变革，产生了深远影响，也给人类的生活带来了翻天覆地的变化。但是网络应用的发展受到安全的威胁，安全问题成为电子政务和电子商务发展的瓶颈。如何保证 Internet 网上信息传输的安全，解决真实性、保密性、完整性和不可否认性的问题，成了现阶段发展的一个重要环节。对称密码技术在解决这些问题时有许多技术的局限，而公开密钥密码克服了这些限制，能够全面解决这些安全问题。

事实上，世界各国为解决 Internet 的安全问题，都进行了多年的研究，初步形成了一套完整的 Internet 安全解决方案，即目前被广泛采用的 PKI(Public Key Infrastructure，公钥基础设施)技术。PKI 技术采用证书管理公钥，通过第三方的可信任机构 CA(Certificate Authority，认证中心)，把用户的公钥和用户的其他标识信息(如名称、e-mail、身份证号等)捆绑在一起，在 Internet 上验证用户的身份。目前，通用的办法是采用建立在 PKI 基础之上的数字证书，通过把要传输的数字信息进行加密和签名，保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。作为一种基础设施，PKI 能够提供一系列的安全服务，满足许多应用的安全需求。目前，PKI 的应用已经深入到许多成熟的应用中，如安全电子邮件、WEB 服务安全、VPN 应用等。

因此能够说 PKI 结构是安全体系架构发展的基础，详尽地分析和研究 PKI 结构对理解和设计安全体系架构具有十分重要的意义。

目前，与 PKI 相关的安全体系架构研究所取得的主要成果有：①Open Group 组织提出的 PKI 体系结构(APKI)。②Intel 安全实验室提出的通用数据安全体系结构 CDSA。③RSA 安全实验室提出并开发的 PKCS#11 模块。

2.2.2　PKI 概念的提出与发展

20 世纪 80 年代，美国学者提出了 PKI 的概念。为了推进 PKI 在联邦政府范围内的应用，美国在 1996 年成立了联邦 PKI 指导委员会；1999 年，PKI 论坛成立；2000 年 4 月，美国国防部宣布要采用 PKI 安全倡议方案；2001 年 6 月 13 日，在亚洲和大洋洲推动 PKI 进程的国际组织宣告成立，它就是“亚洲 PKI 论坛”，其宗旨是在亚洲地区推动 PKI 标准化，为实现全球范围的电子商务奠定基础。

所谓的 PKI，是一种遵循既定标准的密钥管理平台，通过使用公开密钥技术和数字证书，提供密钥和证书管理功能来确保系统信息安全并负责验证数字证书持有者身份的一种体系。

PKI 系统是一个集硬件、软件、人力资源、相关政策和操作规范为一体的综合系统，它由公开密钥密码技术、数字证书、证书发放机构(CA)和关于公开密钥的安全策略等基本成分共同组成。严格地讲，一个完善的 PKI 必须具有认证机构 CA、证书库、密钥备份及恢复系统、证书作废处理系统、PKI 应用接口系统等组成部分，其中，认证机构 CA 是整个系统的核心。用户使用由 CA 签发的数字证书，结合加密技术，可以保证通信内容的保密性、完整性、可靠性及交

易的不可抵赖性，并进行用户身份的识别。PKI 的基础是加密技术，核心是证书服务，其结构如图 2－1 所示。

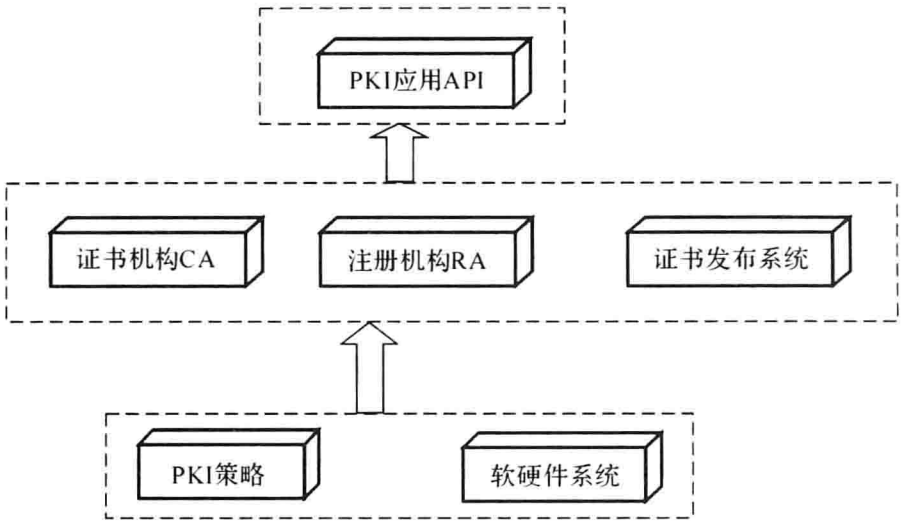

图 2－1　PKI 系统结构图

PKIX(Public－Key Infrastructure Using X.509)是由 IETF 组织中的 PKI 工作小组制定的系列国际标准。此类标准主要定义基于 X.509 和 PKCS 的公钥体系基础框架。PKIX 中定义的 4 个主要模型为用户、认证中心 CA、注册中心 RA 和证书存取库。

到目前为止，虽然各类不同的 CA 机构都遵循 X.509 的标准颁发 CA 证书，但证书的格式和形式都在变化。其中，使用得最多的客户端证书分别派生出了硬件证书(如 USB 证书、IC 卡证书)、软件证书(如安装在电脑中的软件证书)、漫游证书(可从网络上直接下载，方便异地漫游用户)等三类证书，它们的安全性和成本从高到低排列，而易用性则反之，从低向高排列。

2.2.2.1　典型结构和成熟的 PKI 产品

PKI 结构中关键是信任模型 CA 的建立，目前发展比较成熟的结构有以下几种。

1. 严格层次信任模型(见图 2－2)

它是一个主从 CA 关系建立的分级 PKI 结构，根 CA 是整个信任域中的信任锚。终端实体间通过根 CA 来对证书进行认证。

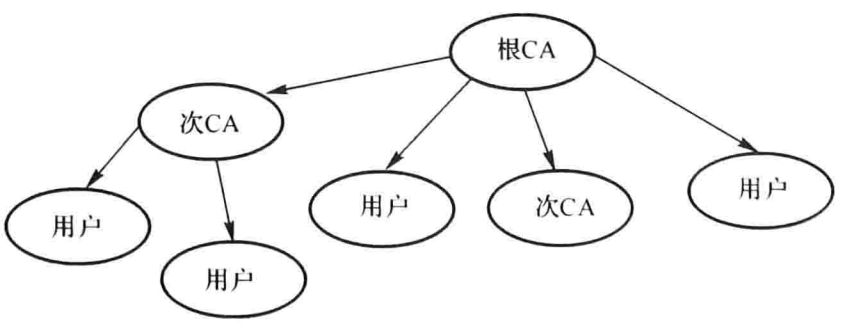

图 2－2　严格层次信任模型

优点：此模型系统结构简单，证书管理易于实现和管理，信任关系可信度高，易扩展。

缺点：根 CA 的安全性要求高，如果根 CA 的私钥泄露，整个信任域的信任关系将瓦解，且容易造成垄断，不易扩展到支持大量群体。

2. 网状信任模型(见图 2-3)

系统中存在多个根 CA,根 CA 间进行交叉认证,不同根的 CA 间也可以建立交叉认证。

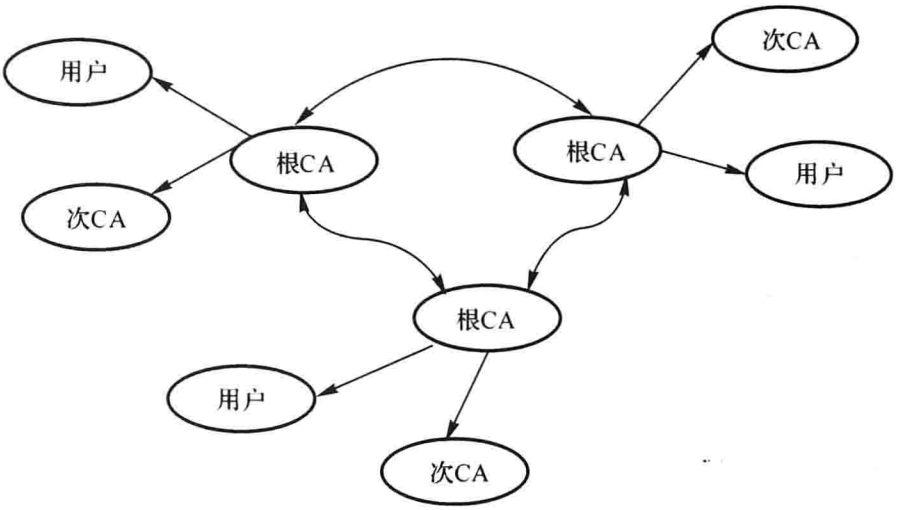

图 2-3　网状信任模型

优点:不同根 CA 的终端实体进行认证时,可选取相同的信任锚;信任路径构造简单。弱安全性的 CA 只影响少量用户,可减少颁发证书的个数。

缺点:信任路径的发现比较困难,用户必须基于证书的内容而非在系统中的位置来确定证书的用途,因此证书会很复杂,扩展性差。

3. 桥信任模型(见图 2-4)

桥 CA 允许终端实体保持原有的信任锚,它不直接向用户颁发证书。对于各根 CA 来说,桥 CA 是同级而不是上级。一个根 CA 与桥 CA 建立交叉认证关系后即可获得构造和验证与桥 CA 连接的其他机构的证书路径的能力。

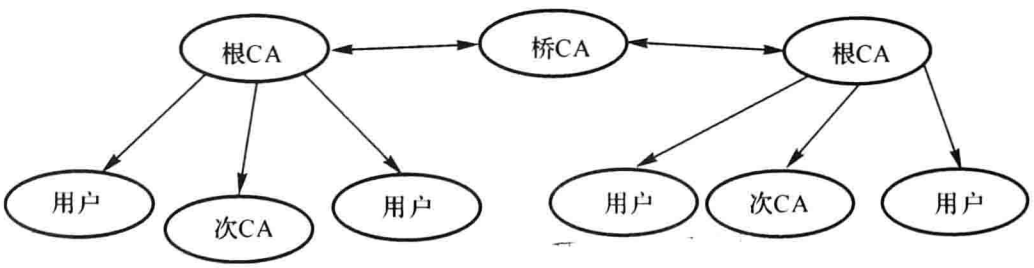

图 2-4　桥信任模型

优点:信任路径唯一,较容易连接现有的 PKI 系统,证书路径发现相对容易。

缺点:如果连接网状模型可能会给路径的有效发现和确认带来麻烦;大型 PKI 的目录互操作性不方便;证书复杂,桥 CA 需要利用证书信息来限制不同 PKI 系统的信任关系。

4. 信任列表模型(见图 2-5)

每个 CA 都是信任锚,其关系是平行的。

优点:方便简单,操作性强;对终端用户要求低。

缺点:安全性差,其中一个 CA 被破坏,其他 CA 的安全性降低;终端用户与根 CA 交互性差;扩展性差,给用户管理带来困难。

目前较为典型的 PKI 体系可分为美国联邦的 PKI 体系和加拿大的 PKI 体系。现分别作

下述介绍。

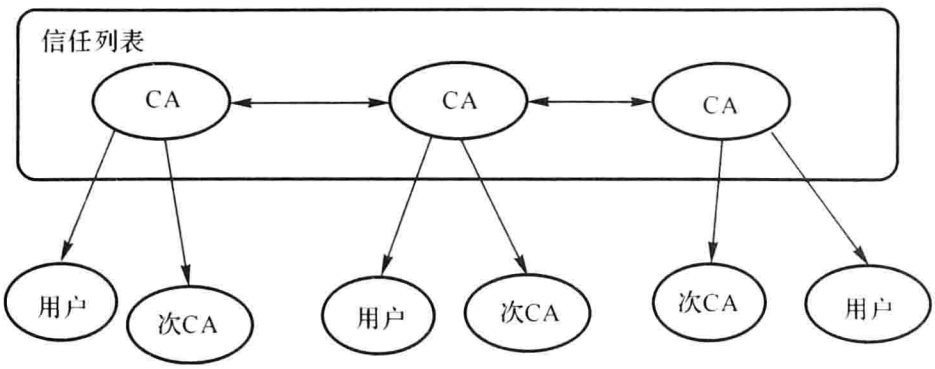

图 2-5　信任列表模型

1. 美国联邦的 PKI 体系(见图 2-6)

美国联邦 PKI 体系主要由联邦的桥认证机构(Federal Bridge CA,FBCA)、首级认证机构(Principal CA,PCA)和次级认证机构(Subordinate CA,SCA)等组成。

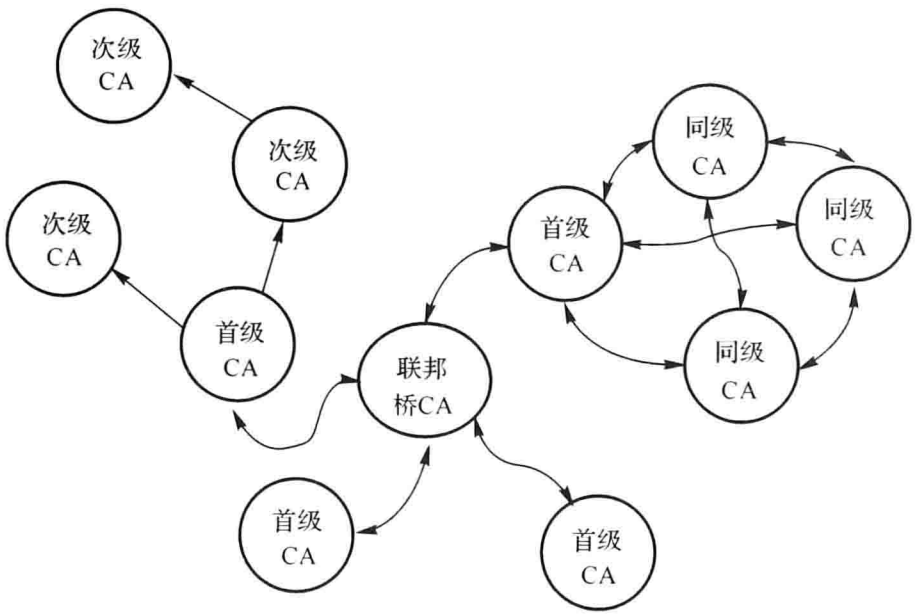

图 2-6　美国联邦 PKI 体系结构

美国联邦 PKI 是自下而上建立的一个庞大 PKI 体系。联邦 PKI 的体系结构中没有采用根 CA,而是采用了首级 CA,这是因为在美国,信任域的结构是多种多样的。联邦政府首先成功地在各联邦机构中分别使用了不同的 PKI 产品,因此它的 PKI 体系结构也是多种多样的,如分级(树状)结构、网状结构和信任列表等等。

PKI 产品的多样性提高了政府机构的工作效率,但也造成了各机构彼此之间难以互操作的问题。为了解决这个问题,联邦政府计划联合各联邦机构中独立的 PKI/CA 共同组建美国联邦 PKI 体系,采用桥 CA 的技术,利用桥 CA 为不同信任域的首级 CA 颁发交叉认证的证书,建立各个信任域的担保等级与联邦桥 CA 的担保等级之间的映射关系,更新交叉认证证书,发布交叉认证证书注销黑名单。联邦的桥 CA 不直接向用户颁发证书,允许用户保留自己的原始信任点。任何结构类型的 PKI 结构都可以通过这个机构连接在一起,实现彼此之间的信任,并将每一个单独的信任域通过联邦的桥 PKI 扩展到整个联邦 PKI 体系中,并且其中的