基于智能卡的 PKI 体系实现框架

曹化工[1] 梁宗炼[1] 高小新[2] 童 敏[3] 欧阳由[3]

[1](华中科技大学 计算机科学与技术学院，湖北 武汉 430074)
[2](华中师范大学 电路与系统研究所，湖北 武汉 430072)
[3](华中科技大学 机械学院，湖北 武汉 430074)

摘 要：在 PKI(Public Key Infrastructure)的基础上，讨论了具有特定格式的数字签名/验证、静态数据鉴别和动态数据鉴别等安全机制，构建了 IC 卡应用系统密钥管理框架，实现了信息的保密性、完整性和不可否认性要求.

关 键 词：非对称加密算法；密钥管理；PKI；静态数据鉴别；动态数据鉴别
中图分类号：TP391 **文献标识码**：A **文 章 编 号**：1000-1220(2003)06-1004-05

Implementation of Smart Card-based PKI Framework

CAO Hua-gong[1], LIANG Zong-lian[1], GAO Xiao-xing[2], TONG Ming[3], OU Yang-you[3]

[1](*School of Computer Science and Technology, Huazhong University of Sciense and Technology, Wuhan* 430074, *China*)
[2](*Institute of Electrocircuit and System, CCNU, Wuhan*, 430072, *China*)
[3](*Mechanical School of Huazhong University of Sciense and Technology, Wuhan* 430074, *China*)

Abstract: In this paper, a set of security mechanisms have been discussed based on PKI, such as digital signature and verification, static data authentication and dynamic data authentication. A framework of secret protection in IC card application system has been implemented to ensure privacy, integrity and accountability of infomations.
Key words: asymmetric crypto algorithm key management public key infrastructure static data authentication dynamic data authentication

1 概 述

信息技术的迅猛发展，特别是计算机技术、网络技术、通信技术和信息安全技术的发展，使人们的生活方式和生产方式发生了深刻的变化. 信息产业部副部长吕新奎在'98 国际电子商务论坛中曾指出：国民经济信息化，企业信息化是基础，金融电子化是保证，信息安全是关键. 高科技在给人们的工作和生活带来方便舒适的同时，也给人们平添了许多困扰，安全问题首当其冲，密钥管理成为信息保密的核心. PKI 被誉为现代信息社会安全的基石，随着电子商务的兴起，PKI 显得日益重要.

PKI 建立在公钥加密算法密码体制基础之上，它简化了密钥管理，节省了密钥在保存、传送方面所花费的代价. 在现代信息社会中 IC 卡扮演着一个不可忽视的角色. IC 卡为密钥的存储管理提供了良好的介质，密钥的产生、保存、分发和更新都有一套严密的安全措施[1]. 它本身有许多优点：安全性高、保密性好、一卡多用、方便小巧. 现已经广泛应用于金融、保险、交通管理、社会保障、安全认证与加密、医疗保健、公共事业收费、电子商务、电子证照等领域.

2 对称加密算法密钥管理

在对称加密算法密钥管理方式中，通讯双方拥有相同的秘密密钥，他们之间的会话就是在这个密钥的基础上进行的. 会话秘密完全寓于秘密密钥之中，密钥的泄漏必将导致整个安全体系的瓦解. 下面以 Kerberos 协议为例说明对称加密算法密钥管理的特点.

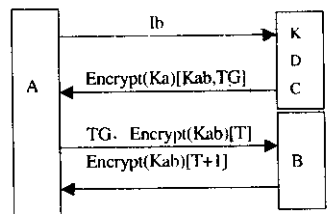

图 1 Kerberos 简化模型
Fig. 1 Kerberos predigested model

图 1 是一个简化的 Kerberos 模型示意图，KDC 为密钥分配中心，具有认证和授权服务的功能，它保存了各个实体的秘密密钥，A、B 为两个实体，Ia、Ib 分别是实体 A、B 的标识符，Ka、Kb、Kab 分别为实 A、B 的秘密密钥和两者之间的会话密钥，T 为时间戳. TG＝Encrypt(Kb)〔Ia，Kab〕就是票据，用来传递 Kab 给实体 B. T 的任务就是在两者之间实现会话通道的建立. 秘密寓于票据之中，A 和 B 并不知道对方的密钥. 整个模型的安全由 KDC 保证，Kab 由 KDC 在通讯请求时产生，通过票据 TG 传递、分发，会话结束后自动销毁. A 和

收稿日期：2002-08-02 作者简介：曹化工，教授. 研究方向为数据库、工作流和系统集成技术. 梁宗炼，硕士研究生. 研究方向为系统集成与信息安全. 高小新，硕士研究生. 研究方向为数据库技术和智能卡系统. 童 敏，教授. 研究方向为智能卡与信息安全技术. 欧阳由，讲师. 研究方向为智能卡与信息安全技术.

B 之间建立通讯联系的过程被简化成图 1 描述的四个步骤.

以上 Kerberos 采用了 KDC 实现密钥的管理,但在 IC 卡系统中采用这种方案不可避免地会妨碍 IC 卡的应用.因为在这种情况下,IC 卡必须与 KDC 联机交互,通过联机和 KDC 认证并取得会话密钥,用于后来的交互通讯.况且,每一次的会话都要和 KDC 建立联系,如果有很多会话实体还会造成通讯瓶颈.

IC 卡应用采用了一个比较巧妙的方法,既实现了对称加密算法密钥管理,又避免了建立 KDC,优化了整个系统体系,方便了 IC 卡的应用.如图 2 所示,K 为母卡主密钥,ID_{IC}为 IC 卡标识符,K_{IC}为IC卡主密钥,且$K_{IC}=3DES(K)[ID_{IC}]$.总的思路是密钥分散,即母卡通过使用自身携带的密钥 K,对 IC 卡的唯一标识号 ID_{IC}进行 3DES 加密,得到的子密钥 K_{IC}作为 IC 卡的主密钥.在进行加密信息传递应用时,IC 卡使用主密钥 K_{IC}对信息进行加密后,密文传递给终端;终端为了解密密文首先从 IC 卡取得其标识符 ID_{IC},接着用 SAM 卡密钥 K(即保存到 SAM 卡中的母卡主密钥)作分散运算得 K_{IC},然后终端使用密钥 K_{IC}解密密文得到信息.IC 卡并没有向终端传递 K_{IC},而是传递 ID_{IC},K_{IC}在 SAM 卡内部生成,IC 卡和终端 SAM 卡拥有共同密钥 K_{IC}进行信息传递.IC 卡应用系统就是通过这种分散方式,经过多级分散,形成一个密钥体系,管理和应用就以该体系为基础予以实现.密钥体系的顶级密钥是明文的,分散保护了顶级明文密钥,使得系统更为安全,分散了风险,在下一级密钥被攻破后,对上一级密钥基本没有影响,从而在一定限度内保护了同级的其他应用卡.

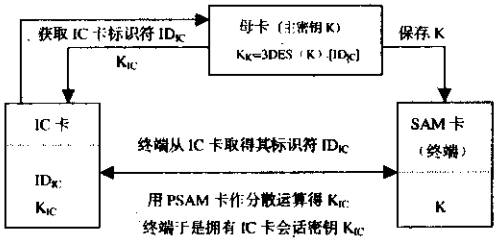

图 2　对称加密算法密钥管理实现

Fig. 2　The realization of secret management with symmetric crypto algorithm

对称加密算法密钥管理具有速度快和易于实现的优点,但是不具备防抵赖的能力.而实现防抵赖是电子商务应用中信息交互的基本要求之一,非对称加密算法密钥管理能很好地解决这个问题.

3　非对称加密算法密钥管理

在非对称加密算法密钥管理中,每个实体拥有一对密钥.整个管理系统拥有一个认证中心 CA,它负责实体身份的认证、实体的注册、公钥的登记、公钥证书的发放注销和纠纷的仲裁等.

3.1　PKI 协议简化模型

PKI 建立在公钥密码体制基础之上,它提供了一套适合于分布式网络环境通讯双方之间的认证策略[2,3,4].下面通过

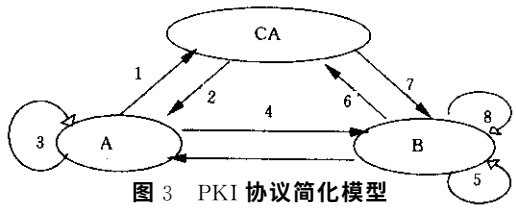

图 3　PKI 协议简化模型

Fig. 3　PKI Protocol Predigested Model

模型(如图 3)讨论实体 A 与实体 B 之间如何建立安全通讯连接.其中,PK_{CA}为 CA 公钥,$Cert_A$ 为 A 证书,$Cert_B$ 为 B 证书,K_{SES}为会话密钥,Msg 为消息.

步骤:

1. A 向 CA 发出与 B 通讯的请求;

2. CA 把 B 的公钥证书交给 A,A 用 CA 公钥对 B 的证书进行认证得到 B 的公钥;

3. A 生成会话密钥 K_{SES};

A 对 Msg 作 Hash 运算得到 H=Hash[Msg];

A 用 K_{SES}对欲发送的信息 Msg 和 H 作加密运算得到 $C=Encrypt(K_{SES})[Msg,H]$;　A 用私钥 SK_A 对 K_{SES}进行签名得到 $S=Sign(SK_A)[K_{SES}]$;

A 用 B 的公钥 PK_B 加密 S 得到 $E=Encrypt(PK_B)[S]$;

4. A 把 C 和 E 一起传递给 B;

5. B 获得 A 传来的 C 和 E,并用私钥 SK_B 解密 E 得到的 S;

6. B 向 CA 发出获取 A 证书的请求;

7. CA 把 A 的公钥证书交给 B,B 用 CA 公钥对 A 的证书进行认证得到 A 的公钥;

8. B 使用 A 的公钥 PK_A 校验签名 S 得到 $K_{SES}=Verify(PKA)[S]$

并用 K_{SES}解密 C 得到 Msg 和 H,[Msg,H] = $Decrypt(K_{SES})[C]$

计算 H′=Hash[Msg],比较 H′和 H 验证 Msg 的完整性

3.2　PKI 在智能卡应用中的实现问题分析

将 PKI 模型应用到 IC 卡中时,必须根据 IC 卡具体的应用环境作适当的取舍.IC 卡有特殊的环境要求,所以 PKI 在 IC 卡应用中的实现尚需解决一些特殊问题.整个 IC 卡应用系统是由认证中心 CA、发卡方、终端、安全认证卡 SAM 和用户卡几个部分组成的.终端可以支持多个应用系统,它要保存所有被其支持的应用系统 CA 公钥,终端上使用的 SAM 卡和用户卡要保存相应的 CA 公钥索引.在用户卡与终端交互过程中,不需要 CA 参与,建立交互的信息均被保存在终端和卡中,所以用户卡和 SAM 卡需要和终端之间进行相应的信息鉴别,以决定卡片和终端的合法性.因此,PKI 在智能卡应用中的实现涉及到这些相关问题:

1. CA 公钥的产生、保存、分发和更新;

2. 发卡方密钥对的产生、保存或更新,公钥证书的生成、保存、分发和更新,公钥证书由 CA 签发;

3. 用户卡、SAM 卡密钥对的生成和保存,公钥证书的生成、保存;公钥证书由发卡方签发;

4. 用户卡、SAM 卡和终端应保存相应的安全信息,用来实现三者之间的校验,同时适应一卡多用和打破行业、区域限制的需求;

5. 用户卡、SAM 卡和终端之间的合法性校验;

6. 合法性校验的内部机制及其实现基础;

7. CA 在发卡和建立交互过程中的作用.

4 基于 IC 卡的 PKI 密钥管理框架

本部分提出了 PKI 密钥管理实现框架,在给出模型的基础上,分别讨论了认证中心 CA 的密钥对生命周期,发卡方、SAM 卡和用户卡密钥对管理等密切相关的问题相关部分参考图 5 和图 6.

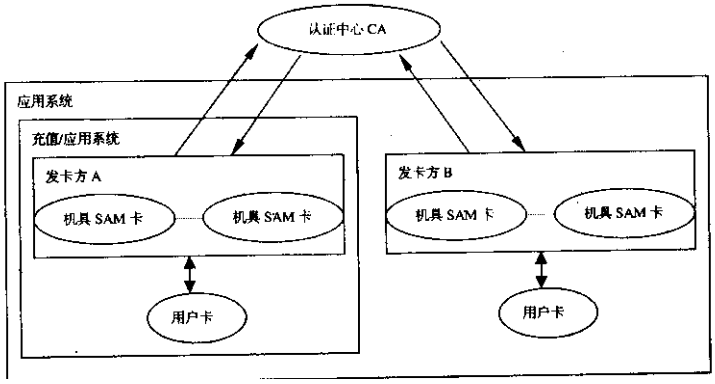

图 4 PKI 密钥管理框架

Fig. 4 PKI key management framework

根据第 3 部分的分析,基于 IC 卡的 PKI 密钥管理框架模型如图 4 所示.

4.1 CA 密钥对的生命周期

1. 规划 应用系统通过对当前 CA 密钥对的安全性进行评估,确定新引入的密钥对的模长和使用期限等其它属性.

2. 生成 评估后如果有必要引入新的密钥对,则要生成预期的新的 CA 密钥对,保存在特定装置中.

3. 分发 CA 必须把生成的公钥分发给整个应用系统的发卡方及其终端.确保数据的完整性和 CA 公钥的一致性.

4. 使用 CA 私钥用于为发卡方公钥生成证书,CA 公钥用来鉴别发卡方公 钥证书.

5. 更新 对达到使用期限或其安全性受到破坏的 CA 密钥对,应用系统要进行密钥更新,以适应新的规划要求.

4.2 发卡方和用户卡密钥管理

1. 发卡方 A 向 CA 请求注册:CA 为发卡方 A 产生密钥对,CA 备份密钥对并将其保存在特定装置中;

2. CA 向发卡方 A 颁发证书:CA 用自己的私钥对 A 的公钥进行签名产生数字证书,传给 A 保存起来,在用户卡注册时分发;

3. 用户卡向发卡方 A 注册:发卡方 A 为用户卡生成密钥对,保存在用户卡卡中;

4. 发卡方 A 向用户卡颁发证书:发卡方 A 用自己的私钥对用户卡公钥进行签名产生数字证书,传给用户卡保存在卡中;

发卡方 SAM 卡、终端和用户卡,在 CA 分发阶段装入 CA 公钥或其索引,并保存起来;在 CA 更新阶段更新 CA 公钥,并重新由 CA 注册.

5 签名/校验机制

签名/校验机制是 PKI 体系的基础,公钥证书的生成和校验、静态数据鉴别和动态数据鉴别等安全机制均是在它的基础上实现的.它是理解 PKI 体系的关键.

5.1 签 名

给定私钥 SK(模数长 N 字节)和报文 MSG(L 字节,$L > N - 22$),计算签名 S.

1. 计算 MSG 的 Hash 值 H(20 字节).

$H = Hash[MSG]$

2. 将 MSG 分成 MSG_1 和 MSG_2 两部分.

$MSG = (MSG_1 || MSG_2)$

其中 —— MSG_1 由最左边 N-22 字节组成

—— MSG_2 由其余 $L - (N - 22)$ 字节组成

3. 定义字节

$B = '6A'$

4. 定义字节

$E = 'BC'$

5. 定义数据块 X(N 字节).

$X = (B || MSG_1 || H || E)$

6. 计算签名 S(N 字节).

$S = Sign(SK)[X] := X^d \bmod n$

签名 S(报文 MSG 的证书)不能单独使用,因为它包含的信息并不完备.如果同时获得签名 S 和它的配套数据(报文余留 MSG_2),只要知道与私钥 SK 对应的公钥 PK,就可以校验签名的正确性并复原报文 MSG.

5.2 校 验

给定公钥 PK(模数长 N 字节)、签名 S 和它的配套数据

(报文余留 MSG2),检验签名 S 的正确性.

1. 检查签名 S 的长度是否为 N 字节.
2. 计算数据块 X(N 字节).

$X = Verify(PK)[S] := S^e \bmod n$

3. 将 X 分成 B、MSG_1、H 和 E 四部分.

$X = (B \,||\, MSG_1 \,||\, H \,||\, E)$

其中 —— B 的长度为 1 字节
—— H 的长度为 20 字节
—— E 的长度为 1 字节
—— MSG_1 由其余 N-22 字节组成

4. 检查字节 B 是否为 '6A'.
5. 检查字节 E 是否为 'BC'.
6. 计算 $MSG = (MSG_1 \,||\, MSG_2)$
检查是否满足 $H == Hash[MSG]$,若是,报文合法.

6　静态数据鉴别机制

终端使用基于公钥技术的数字签名/鉴别机制进行静态数据鉴别,以验证驻留在 IC 卡中的静态数据的合法性.目的在于判断 IC 卡个人化后数据是否在未授权的情况下发生改变.[7]

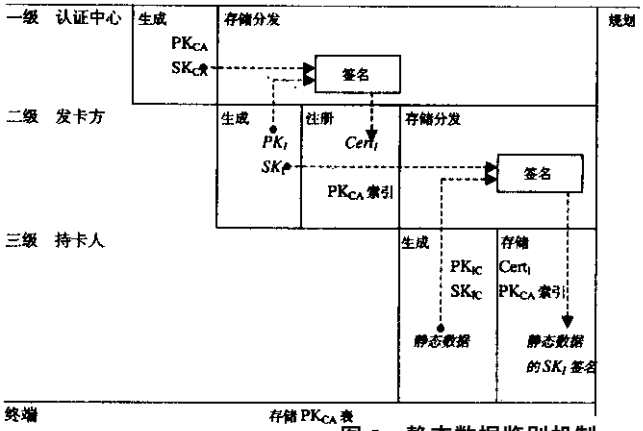

图 5　静态数据鉴别机制

Fig. 5　Static Data Authentication

IC 卡提供给终端:
—— PK_{CA}索引
—— PK_I 证书 $Cert_I$
—— 静态数据 SK_I 签名

终端:
—— 从 PK_{CA}表找到 PK_{CA}
—— 使用 PK_{CA}校验 $Cert_I$
—— 使用 PK_I 校验静态数据签名

终端首先从 IC 卡取得 PK_{CA}索引,从 PK_{CA}表找到 PK_{CA};再从 IC 卡取得 SK_{CA}签名的 PK_I 证书 $Cert_I$,用 IC 卡指定的 PK_{CA}进行校验;然后从 IC 卡取得静态应用数据的 SK_I 签名,用 PK_I 进行校验.校验成功则认为终端是合法的.

7　动态数据鉴别机制

终端使用基于公钥技术的数字签名/鉴别机制进行动态

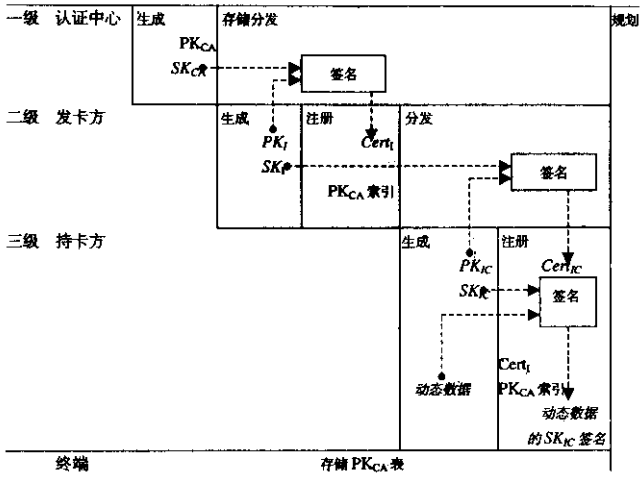

图 6　动态数据鉴别机制

Fig. 6　Dynamic data authentication

数据鉴别,以验证驻留在 IC 卡中的动态数据和从终端接收的动态数据的合法性.目的在于认证 IC 卡.

IC 卡提供给终端:	终端:
——PK_{CA}索引	——从 PK_{CA} 表找到 PK_{CA}
——PKI 证书 $Cert_I$	——使用 PK_{CA} 校验 PKI 证书 $Cert_I$
——PK_{IC} 证书 $Cert_{IC}$	——使用 PKI 校验 PK_{IC} 证书 $Cert_{IC}$
——卡和终端动态数据	——使用 PK_{IC} 校验动态数据签名

终端首先从 IC 卡取得 PK_{CA} 索引,从 PK_{CA} 表中找到 PK_{CA};再从 IC 卡取得 SK_{CA} 签名的 PKI 证书 $Cert_I$,用 IC 卡指定的 PK_{CA} 进行校验;然后从 IC 卡取得 SK_I 签名的 PK_{IC} 证书 $Cert_{IC}$,用 PK_I 进行校验;最后 IC 卡生成动态应用数据的 SK_{IC} 签名,送给终端用 PK_{IC} 进行校验.如校验成功则认为 IC 卡是合法的[7].

8 结 束 语

本文初步将 PKI 的有关原则和策略在 IC 卡的环境限制中予以实现,使之符合 IC 卡的要求,在 IC 卡中实现非对称加密算法密钥管理.在此密钥管理构架下,实现了一套确定格式的数字签名/验证、静态数据鉴别、动态数据鉴别等安全机制,实现了信息交互的保密性、完整性和不可否认性要求,为 IC 卡应用提供了安全保证.

References:

1 Yacobi Y. On the continuum between on-line and off-line e-cash systems[C]. Financial Cryptography′97. Anguilla, British West Indies: Springer-Verlag, 1997:193～202.

2 Schneier B. Applied cryptography protocols, algorithms, and source code in C, Second edit[M]. Beijing: Machine Indastry Press. 2000,1

3 Sun Xiao-rong, Wang Yu-min. Authentication and key distribution protocol for distributed computer environment[J]. Chinese J. Computers, 1999, 22(6):577～581.

4 Lu Yu. Li Yong-qi. Model of intranet authentication based on digital signature &. smart card[J]. Computer Engineering &. Applications, 1999(3):107～109.

5 Schnopr C P. Efficient identification and signaure for smart cards [C]. In: Advances in Cryptology-CRYPTO′89. Santa Barbara, 1985:239～252.

6 Lein. H. New digital signature scheme based on discrete logarithm [J]. Electron lett, 1994, 30(5):36～40

7 Europay Mastercard and Visa Workgroup. EMV2000 Integrated circuit card specification for payment systems(Book2 - Security &. Key Management)[J]. 2000,12 :43～50

附中文参考文献:

2 (美)施奈尔(Schneier. B.)著. 应用密码学:协议、算法与 C 源程序[M]. 第二版. 吴世忠等译,何德全校[M]. 北京:机械工业出版社,2000,1:200～204

3 孙晓蓉,王育民. 计算机分布式环境中的认证与密钥分配研究[J]. 计算机学报,1999,6,22(6):577～581

4 卢昱,李勇奇. 基于数字签名及智能卡的 Intranet 认证模型[J]. 计算机工程与应用,1999,3:107～109

基于智能卡的PKI体系实现框架

作者： 曹化工， 梁宗炼， 高小新， 童敏， 欧阳由

作者单位： 曹化工,梁宗炼(华中科技大学,计算机科学与技术学院,湖北,武汉,430074)， 高小新(华中师范大学,电路与系统研究所,湖北,武汉,430072)， 童敏,欧阳由(华中科技大学,机械学院,湖北,武汉,430074)

刊名： 小型微型计算机系统 ISTIC PKU

英文刊名： MINI-MICRO SYSTEMS

年，卷(期)： 2003,24(6)

参考文献(10条)

1. 孙晓蓉;王育民 计算机分布式环境中的认证与密钥分配研究[期刊论文]-计算机学报 1999(06)

2. 施奈尔;吴世忠;何德全 应用密码学:协议、算法与C源程序 2000

3. Europay Mastercard;Visa Workgroup EMV2000 Integrated circuit card specification for payment systems(Book2 - Security & Key Management) 2000(12)

4. LeinH New digital signature scheme based on discrete logarithm[外文期刊] 1994(05)

5. Schnopr C P Efficient identification and signaure for smart cards 1985

6. Lu Yu;Li Yong-qi Model of intranet authentication based on digital signature & smart card 1999(03)

7. 卢昱;李勇奇 基于数字签名及智能卡的Intranet认证模型 1999

8. Sun Xiao-rong;Wang Yu-min Authentication and key distribution protocol for distributed computer environment[期刊论文]-Chinese Journal of Computers 1999(06)

9. Schneier B Applied cryptography protocolsalgorithmsand source code in CSecond edit 2000

10. Yacobi Y On the continuum between on-line and off-line e-cash systems Financial Cryptography97 1997

引证文献(3条)

1. 黄成.汪海航 智能卡在WPKI中的应用研究[期刊论文]-计算机技术与发展 2007(12)

2. 焦华清.覃征 PKI智能卡在网上报税系统中的应用[期刊论文]-金卡工程 2006(5)

3. 朱洪德 血液生化分析系统中统计分析及安全加密的研究与实现[学位论文]硕士 2006