智能密码钥匙

——原理、技术及应用

Cryptographic Smart Token: Principles, Techniques and Applications

飞天诚信科技股份有限公司◎编著

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

飞天诚信科技股份有限公司
智能网络身份认证北京市工程实验室

智能密码钥匙
——原理、技术及应用

飞天诚信科技股份有限公司　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书总结了上市公司“飞天诚信”（深圳创业板）历年来积累的心得体会，综合介绍了智能密码钥匙的应用案例、技术方案、体系架构、安全机制等多个方面的知识，展现了飞天诚信对于智能密码钥匙的深厚积累和独到的认识。具体内容包括智能密码钥匙发展沿革，智能密码钥匙基础知识，智能密码钥匙产品形态，智能密码钥匙应用案例，新一代智能密码钥匙，智能密码钥匙设计开发，以及智能密码钥匙关键技术。

本书可以作为开发智能密码钥匙的工程技术人员和采购使用智能密码钥匙的用户及集成、开发者的参考书。

图书在版编目（CIP）数据

智能密码钥匙：原理、技术及应用 / 飞天诚信科技股份有限公司编著. — 北京：电子工业出版社，2015.7
ISBN 978-7-121-26063-6

Ⅰ. ①智… Ⅱ. ①飞… Ⅲ. ①密钥学 Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字（2015）第 100185 号

策划编辑：窦 昊
责任编辑：窦 昊　　特约编辑：王 崧
印　　刷：北京中新伟业印刷有限公司
装　　订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×980　1/16　印张：19.75　　字数：455 千字
版　　次：2015 年 7 月第 1 版
印　　次：2015 年 7 月第 1 次印刷
定　　价：69.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010)88258888。

编 委 会

序　言

中央网络安全和信息化领导小组的成立标志着中国网络安全和信息化工作进入了一个崭新的阶段，习近平总书记关于网络安全和信息化的系列论述全面提升了国家战略层面的认识高度，而目前复杂多变的网络空间博弈则在很大程度上改变了信息安全的格局，也对信息安全提出了新的和更高的要求。

近一阶段以来，自主可控成为信息安全领域的一大热点话题，并形成了国家倡导推动，科研、企业和行业广泛参与，用户逐渐认可的发展态势。人们意识到，保障重要信息系统和国家关键基础设施的安全，离不开自主可控的信息和安全技术。而要真正实现自主可控，却并不是一件容易的事情，需要扎实的积累和大胆的创新才能有所突破。可喜的是，这些产品技术正在不断增多。

智能密码钥匙是一种被广泛使用的便携型密码设备。它结构较为简单，技术较为成熟，具备在自主可控方面率先取得突破的潜力。不仅如此，智能密码钥匙既是密码算法的载体，同时也是信息安全系统的组成部分，在金融、政务等重要领域得到广泛应用，兼具多重特性，有望成为推动自主可控的信息安全保障体系普及应用的有力抓手。令人欣喜的是，在工业和信息化部、国家密码管理局、中国人民银行等相关部门的协作推动下，以飞天诚信为代表的一批企业已经掌握自主知识产权的核心技术，采用自主安全芯片作为硬件平台，推出了一批具有市场竞争力的智能密码钥匙产品，这是自主可控方面的一个积极和有效的探索。

飞天诚信将自己在智能密码钥匙方面的心得体会整理出版，有助于社会和大众更加了解自主密码技术及其应用，不仅能够带动智能密码钥匙行业的技术进步，也与当前信息安全的智能化趋势相吻合。

希望本书的出版能让读者更多地关注智能密码钥匙以及由此引致的自主可控信息安全技术体系，能够带动更多的新生力量对此产生兴趣，进而投身到自主可控的信息技术创新事业中来，共同为国家网络强国战略贡献聪明才智。同时也希望这一技术成果在应用过程中能够继续完善改进，更上一层楼，取得更多更大的成果。

中国工程院院士

前　言

根据密码行业技术指南 GM/Z 0001—2013《密码术语》的定义，智能密码钥匙是“实现密码运算、密钥管理功能，提供密码服务的终端密码设备，一般使用 USB 接口形态”。利用内置的安全机制和密码算法，智能密码钥匙能够实现密钥生成和安全存储、数据加密、数字签名等功能。智能密码钥匙具有“密钥不出设备”的特点，与密钥相关的运算过程在设备内部完成，仅输出运算结果。作为当前安全强度最高的便携式密码设备之一，智能密码钥匙发挥着难以替代的作用，广泛应用于网上银行、电子商务、电子政务、企业办公等领域。

本书总结了飞天诚信科技股份有限公司历年来积累的心得体会，综合介绍了智能密码钥匙的应用案例、技术方案、体系架构、安全机制等多个方面的知识，展现了飞天诚信科技股份有限公司对于智能密码钥匙的深厚积累和独到的认识。自 1998 年成立以来，飞天诚信科技股份有限公司在智能密码钥匙领域辛勤耕耘，创下了业内多项纪录。本书以飞天诚信科技股份有限公司的深厚底蕴为立足点，广泛参考相关研究成果，较为全面地梳理了智能密码钥匙相关的知识体系，从工作原理、技术方案、应用案例到标准规范都有所涉足，内容充实，细节丰富。具体内容包括：

- 智能密码钥匙发展沿革：回顾智能密码钥匙的发展历史。
- 智能密码钥匙基础知识：简要介绍解智能密码钥匙所需的知识。
- 智能密码钥匙产品形态：介绍各种智能密码钥匙产品及其特点。
- 智能密码钥匙应用案例：介绍智能密码钥匙的应用场景。
- 新一代智能密码钥匙：介绍新一代的智能密码钥匙。
- 智能密码钥匙设计开发：介绍智能密码钥匙的体系架构、安全机制及编程开发接口。
- 智能密码钥匙关键技术：介绍智能密码钥匙的核心技术及其方案。

本书是国家规划布局内重点软件企业飞天诚信科技股份有限公司，试图普及智能密码钥匙相关知识，促进智能密码钥匙应用推广，带动行业技术水平提升的心意之作。作为行业内首家建立北京市科协院士专家工作站及北京市工程实验室、持有超过 600 件国内外发明专利、行业内金融领域客户数量最多的上市企业，飞天诚信科技股份有限公司秉承“诚信、务

实、坚持、创新”的文化理念，矢志不渝地为更广泛的行业和企业客户提供安全可靠的基于自主核心技术的智能密码钥匙产品与解决方案。

本书得到了飞天诚信科技股份有限公司各位领导的大力支持及众多同仁的热情帮助：技术服务、知识产权、技术研发等多个部门提供了丰富而翔实的内容；张静、才冬雪、冯文等同事参与了撰写、修改、统稿及校对工作，张一飞、张利琴、付海洋等同事对书稿进行了审核和反馈。衷心感谢各位同事的辛勤工作。

作者是飞天诚信科技股份有限公司的普通员工，水平和眼界有限，难免出现错漏之处，还请各位读者不吝指正。

目　录

第1章

智能密码钥匙发展沿革

1.1 智能密码钥匙的起源

智能密码钥匙顺应科技发展之势而生，因应用需求而成，在市场竞争环境下“野蛮生长”。智能密码钥匙在发展过程中长期缺乏统一的名称，就是因为产品推出在先，而在领域中的统一概念形成在后。出于同样的原因，关于智能密码钥匙的起源也众说纷纭。

一种说法是智能密码钥匙起源于加密锁。加密锁是用来防止软件盗版的硬件产品，其应用方式是在被保护软件的代码中加入检测加密锁是否存在、利用加密锁进行加密运算等与加密锁相关的代码，使得软件脱离加密锁便无法正常运行，以此来达到保护软件不被盗版的目的。如图 1.1 显示了一种加密锁。为了满足防盗版、防破解的要求，加密锁具备了密码运算功能、访问控制、身份鉴别等安全机制，以及“密钥不出设备”的安全特性。随着网络的普及和软件应用及销售模式的改变，用户购买的软件不一定在本地计算机上安装运行，而是将要处理的数据通过网络传到专门运行该软件服务的应用服务器上处理，再通过网络取得数据处理的结果。相应地，软件开发商通过提供该应用服务收取软件费用。在这样的应用模式下，软件供应商面临的问题不再是如何防止软件被复制，而是如何确认网络用户的身份和用户数据的安全。为了满足这一需求，一些加密锁开发者先后推出了可用于存储密钥和识别用户身份的 USB 接口硬件设备，在此基础上逐渐形成了智能密码钥匙产品。

图 1.1 加密锁

另外一种说法是智能密码钥匙起源于智能卡。智能卡是 IC 卡（Integrated Circuit Card，集成电路卡）的一种。IC 卡是将集成电路芯片镶嵌于塑料基片中封装而成的。按照内置芯片类型不同，IC 卡可分为存储卡、逻辑加密卡、CPU 卡等。其中，CPU 卡又称智能卡，卡内的集成电路包括中央处理器（CPU）、可编程只读存储器（EEPROM）、随机存储器（RAM）和只读存储器（ROM），能够固化并运行片内操作系统（Chip Operating System，COS），具备较强的运算能力。其中，实现密码运算和密钥管理的智能卡在密码行业称为智能 IC 卡。根据通信方式的不同，可将智能卡分为以下三类：

- 接触式：通过读写设备的触点与智能卡的触点接触后进行数据的读写。国际标准 ISO/IEC 7816 对此类卡的机械、电气特性等进行了规定。
- 非接触式：读写设备与智能卡没有电路接触，而是通过非接触式的读写技术进行读写。国际标准 ISO/IEC 10536 和 ISO/IEC 14443 系列阐述了适用于此类卡的规定。
- 双界面式：将接触式智能卡与非接触式智能卡组合到一张卡片中，操作相互独立，但可以公用 CPU 和存储空间。

在智能密码钥匙的发展过程中，的确出现过“智能密码钥匙＝智能卡＋读卡器”的说法。而智能卡领域的大量技术及标准被智能密码钥匙产品所使用，也是客观存在的情况。例如，二者的处理器芯片基本是相同的，该芯片被业内通称为智能卡芯片（这也为智能密码钥匙来源于智能卡的说法提供了佐证）；片内操作系统方面，智能卡国际标准 ISO/IEC 7816-4 所定义的 APDU（Application Protocol Data Unit，应用协议数据单元）被智能密码钥匙产品广泛用作指令格式规范；等等。然而，密码运算只是智能卡支持的功能之一，智能卡的功能和用途并不局限于密码设备。图 1.2 显示了一种智能卡。

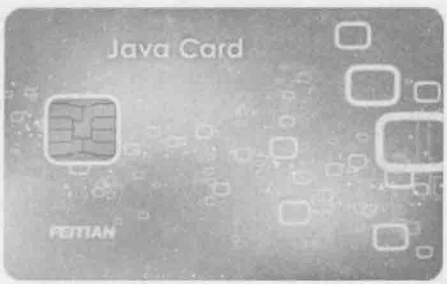

图 1.2　智能卡

到底哪种说法更加合理，如今已不可考。但可以确定的是，这两种产品都给其后诞生的智能密码钥匙打下了深深的烙印。加密锁的安全特性和智能卡的体系结构，都在智能密码钥匙产品中有所继承和体现。

时至今日，智能密码钥匙、智能卡、加密锁这几种同样以安全芯片为核心的产品早已泾渭分明，各有所长：智能卡的功能和用途不局限于密码运算，在电信、交通、金融等众多领域大展拳脚；加密锁紧跟版权保护市场需求，锁内运行外部代码、内置时钟等特色鲜明的功能和配置不断涌现；而智能密码钥匙则兼具高强度的密码运算功能和轻巧便携的产品形态，在“安全”与“易用”之间取得了成功的平衡，成为被广泛认可和使用的一种商用密码设备。

1.2　萌芽时期：1985—2001 年

在萌芽阶段，智能密码钥匙尚未与加密锁或智能卡完成分化，产品形态尚不明确，在市场宣传中往往顶着“USB 接口的智能卡”、“能用作身份认证的加密锁”之类似是而非的名头。例如，《电脑编程技巧与维护》杂志 2001 年第 10 期刊登了一篇名为“智能卡＋读卡器＝ePass”的文章，其中就有这样的叙述：

随着智能卡在银行、社保、安全、支付等诸多领域中的发展应用，建立一个方便的智

能卡的读写设施显得尤为需要。与个人计算机方便连接的智能卡读卡器将是仅次于 GSM 手机的智能卡的最主要的平台。

ISO 7816 是智能卡的标准，但在标准制定之初，没有考虑智能卡与个人计算机的整合，个人计算机也没有 USB 标准接口。1996 年，由微软等几家公司领导建立了个人计算机/智能卡（PC/SC）工作组，其目的是将智能卡整合到操作系统中。为了建立智能卡与个人计算机的结合需要，飞天诚信科技有限公司开发了两款基于USB接口具有智能卡功能的产品。

ePass 1000 是一个钥匙大小的具有智能卡功能的硬件设备，它通过 USB 接口与个人计算机相连，其内部有一个 CPU 控制芯片，可以说它与智能卡一样安全。它支持主要的 PKI 标准，如 CSP 和 PKCS#11。因为它将智能卡与读卡器整合在一个设备中，因此不需要特殊读卡器硬件，只需一个空闲的 USB 端口，在价格上有很大的优势。

再看 2001 年的厂商新闻稿：

飞天诚信科技有限公司于 2001 年 6 月 6 日至 9 日在北京国际贸易中心参加了第四届中国国际智能卡博览会，展位不算太起眼，却给业内带来不小的震动。

专业的展会必然带来比较专业的观众，特展位固然格外引人注目，但在我公司展位前，却吸引了比特展位更多的人流——我公司新推出了 ePass 2000，不需读卡器的智能卡，使用 USB 接口（区别于以往名片一样的外形），可系于钥匙扣上，能真正有效解决电子商务和电子政务中的安全问题，理所当然成为本次展会耀眼的亮点。不少摄像机和记者凑近展柜，纷纷拍下样品的玲珑靓影。

“USB 智能卡，你不心动吗？你知道它会带来什么样的变革吗？”各参展商和客商也交头接耳，仿佛在议论一场即将面临的风暴。戏剧性的是，场外论坛上的精英们还在大讲着 USB 接口钥匙是未来的发展方向。

在此阶段，参与市场竞争的企业以国外智能卡厂商为主，例如，阿拉丁（Aladdin）、金邦达（Gemplus）、RSA、捷德（G&D）等，应用接口等相关标准也普遍采用国际标准。与此同时，一些自主企业也悄悄地进入了这个市场：

- 1985 年，北京大明五洲科技有限公司成立。这是智能密码钥匙领域最早成立的自主企业。
- 1992 年，深圳市明华澳汉科技股份有限公司成立。
- 1998 年，北京飞天诚信科技有限公司（现名飞天诚信科技股份有限公司）成立。
- ……

2001 年，深圳明华澳汉科技股份有限公司取得了国家密码管理局签发的首张智能密码钥匙商用密码产品型号证书，产品型号为 SZD12，标志着这种新的商用密码产品形态得到了国家密码主管机构的确认。

1985—2000 年间，多家涉足智能密码钥匙研发及销售的公司先后成立。刚起步时往往

是“十几个人，七八条枪”，无论是规模还是技术水平等各方面都与国外的“大鳄”相差甚远。例如，2002 年的新闻稿“新年到，喜迁新址，鲤鱼要把龙门跳”中有如下描述：

IT 的寒冬丝毫没有影响飞天疾进的步伐，在其他 IT 公司一片倒闭、裁员、转型声中，飞天公司反而越发壮大，不但继续招兵买马扩充实力，而且开发部喜迁“新居”。

飞天公司开发部由现在的三层 5303 室迁至二层，新的办公场所面积扩大了 1 倍，这正迎合了飞天的发展规划。在此，我们衷心地希望飞天的新老客户继续关注飞天，支持飞天。

但这是民族企业在此领域参与竞争的开始。随着市场规模的扩大，竞争者不断加入，陆续有失败者在激烈的市场竞争中黯然离场。然而，通过残酷的市场竞争，它们中间的幸存者不断成长，变得强大起来，最终有了与国外对手一较短长的底气和雄心。

1.3 混沌时期：2001—2005 年

由于产品先于概念而生，智能密码钥匙自诞生之初就缺乏统一的标准。在发展和应用的过程中，智能密码钥匙甚至一度连统一的名称都没有，被冠以 USB Key、USB Token、U 盾、USB 安全钥匙、U 宝、电子钥匙等多种称呼。名称尚且如此，技术方面鱼龙混杂、良莠不齐也就可想而知了。在混沌阶段，多种技术路线在智能密码钥匙产品得到了应用和推广。经过市场的竞争和应用的选择，优胜劣汰，智能密码钥匙的特征得以逐渐明确，走向一致。

在智能密码钥匙发展初期，曾经出现过“存储型 USB Key”。这种产品以普通单片机芯片为核心，相比智能卡芯片硬件成本较低，但安全防护水平不高；通常不具备生成非对称密钥对的功能，密码运算功能难以满足 PKI 应用需求；尽管可以通过固件开发实现密码算法，但复杂程度高、性能差、维护困难，开发成本高。随着智能卡芯片普及后价格不断下降，“存储型 USB Key”的硬件成本优势逐渐消失，而功能和性能难以满足应用需要及安全强度不满足准入资质要求的硬伤始终无法解决，最终被市场淘汰。

与此同时，源自智能卡国际标准 ISO/IEC 7816 的个人识别码（PIN）成为智能密码钥匙普遍采用的身份鉴别机制。PIN 和智能密码钥匙设备构成了 PKI 应用中的双因素身份认证体系。只有持有智能密码钥匙设备并知道对应的 PIN，才能使用设备中的密钥。如果 PIN 泄露，只要设备本身不被盗用，就还是安全的。类似地，如果设备丢失，如果 PIN 没有泄露，设备中的密钥仍不会被盗用。

由此，智能密码钥匙的特征逐渐确定，具体包括：

- USB 接口，内置安全芯片。
- 具备密码运算功能，可以生成或导入非对称密钥对。
- 有一定的存储空间，可以存储数字证书等用户数据。
- 有使用者身份鉴别机制（通常是 PIN）。

➢ 配有供其他应用程序调用的软件接口的程序（驱动）。

2005 年的一篇旧文“USB Key 的产生与发展”，体现了智能密码钥匙早期的状况：

目前市场上见到的 USB Key 按照硬件芯片不同，可以分为使用智能卡芯片的和不使用智能卡芯片的两种，按照 CPU 是否内置，加密算法又可以分为带算法和不带算法的 USB Key。一般我们把不带加密算法的称为存储型 USB Key，把带加密算法的称为加密型 USB Key。

USB Key 这个概念最早是由加密锁厂家提出来的。加密锁是用来防止软件盗版的硬件产品，加密锁的概念是使安装在计算机内的应用程序脱离加密锁硬件无法运行来达到保护软件不被盗版的目的。随着网络应用的不断深入和应用软件销售模式的改变，未来的软件用户可能不需要购买软件在本地计算机上安装运行，而是将要处理的数据通过网络上传到专门运行该软件服务的应用服务器上处理，再通过网络取得数据处理的结果，软件开发商通过提供该应用服务收取软件费用。这时，软件厂商面临的问题就不再是如何防止本地软件被复制，而是如何确认网络用户的身份和用户数据的安全。于是加密锁厂商提出了 USB Key 的概念，用于识别用户身份。作为国内最大的软件保护厂家，北京飞天诚信科技有限公司于 2000 年推出了国内第一款 USB Key 产品——ePass 1000。

此后，随着电子商务和 PKI 应用的兴起，数字证书作为确认用户身份和保护用户数据的有效手段越来越被人们所接受。然而数字证书实质上表现为带有用户信息和密钥的一个数据文件，如何保护数字证书本身又成为 PKI 体系中最薄弱的环节。数字证书可以保存在各种存储介质上，如软盘、硬盘等。国内 CA 早期颁发的数字证书都以软盘的形式发放，或者由用户从网络上下载，然后导入系统保存在硬盘上。然而，用软盘保存数据是非常不可靠和不安全的，软盘虽然便于携带，却非常容易损坏，而用硬盘保存数据虽然不容易损坏，但不便于携带，更致命的是不论是用硬盘还是用软盘保存数字证书，都非常容易被复制或被病毒破坏。虽然一般数字证书都带有密码保护，然而一旦证书被非法复制，整个安全系统的安全性就降低到仅仅靠密码保护的级别。于是，专门用于存储秘密信息的 USB Key 就很自然地成为数字证书的最佳载体。

USB Key 厂家将 USB Key 与 PKI 技术相结合，开发出了符合 PKI 标准的安全中间件，利用 USB Key 来保存数字证书和用户私钥，并对应用开发商提供符合 PKI 标准的编程接口如 PKCS#11 和 MSCAPI，以便于开发基于 PKI 的应用程序。由于 USB Key 本身作为密钥存储器，其自身的硬件结构决定了用户只能通过厂商编程接口访问数据，这就保证了保存在 USB Key 中的数字证书无法被复制，并且每个 USB Key 都带有 PIN 码保护，这样 USB Key 的硬件和 PIN 码就构成了可以使用证书的两个必要因子。如果用户 PIN 码被泄露，只要保存好 USB Key 的硬件就可以保护自己的证书不被盗用，如果用户的 USB Key 丢失，获得者由于不知道该硬件的 PIN 码，也无法盗用用户存在 USB Key 中的证书。与 PKI 技术的结合使 USB Key 的应用领域从仅确认用户身份，到可以使用数字证书的所有领域。