第一图书网, tushu007.com

# <<CPK密码体制与网际安全>>

## 图书基本信息

书名：<<CPK密码体制与网际安全>>

13位ISBN编号：9787118059397

10位ISBN编号：7118059390

出版时间：2008-12

出版时间：国防工业出版社

作者：南湘浩

页数：238

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

## 前言

2005年美国总统信息技术顾问委员会（PITAC）提交的一篇《网际安全一优先项目危机》的报告，标志着网际（网络世界或社会）安全新时代的到来。
如果说网络安全的主要任务是以堵漏洞、打补丁为主的被动防护的话，那么网际安全的主要任务则是以建立可信系统为主的主动管理。
主动管理的核心内容是建立证明系统，将信息安全建立在证明系统的基础之上，这就是所谓的可信系统（trusting system）。
这是一项新的任务，过去由于没有合适的示证系统和验证系统，信息安全的原则只能采用“出于好意”，或者采用主体可信的前提假设之上，而网际安全则不同，它建立在“互相怀疑”的基础之上，不允许前提假设下的证明或验证。
这种主要任务和基本原则的变化，首先影响安全的基础理论。
过去以“出于好意”的所有安全协议和标准，需要以“互相怀疑”的基点上重新考虑，如：通信协议和标准、可信计算（包括代码认证）协议和标准等，不得不引起革命性的变化。
今年欧洲密码年会上，James Hughes（2004年国际密码年会执行主席）和北京大学博士研究生关志向大会介绍了基于标识的组合公钥（CPK：Combned Public Key）体制，与会权威专家肯定了CPK体制是新型基于标识的体制。
基于标识的体制，代表着现代密码体制发展的新趋势，受到全世界密码界的关注。
CPK体制和标识认证系统得到了我国高层领导的高度重视，也得到了国家保密局、国家知识产权局等有关部门的大力支持。
国务院信息办和安标委已将CPK体制作为国家标准的基础项目，正式纳入标准化研究计划，国家工业和信息化部给予了企业发展基金补助。
SUN公司已决定，将CPK体制作为Solaris操作系统的一部分。

第一图书网, tushu007.com


## 内容概要

2005年美国总统信息技术顾问委员会（PITAC）提交的一篇《网际安全一优先项目危机》的报告，标志着网际（网络世界或社会）安全新时代的到来。
　本书系统介绍了可信系统主要领域的解决方案，这些领域包括过去无法解决的很多课题，现在却变得容易解决了，如：通信的非法接入、非法软件的运行、印章鉴别系统等。
通过应用举例，读者可以发现由于解决了标识认证这一核心课题，使过去无法解决的很多难题都容易得到解决。
因此，“标识认证”是网际安全的“纲”，起到“纲举目张”的作用。
　CPK密码体制、标识认证、可信逻辑作为可信系统的基础理论和技术，越来越显现其意义。
在酝酿成立国际CPK行业联盟，推进国际标准之际，本书的出版具有特殊意义。
希望本书满足国内外读者的要求，对国际联盟和国际标准有所帮助，并以此促进信息安全从网络安全到网际安全的过渡。

## 作者简介

南湘浩，解放军某部研究员；解放军信息工程大学兼职教授、博士生导师；北京大学计算机科学技术系兼职教授；中国计算机学会理事、信息保密专业委员会顾问；中国人民银行信息安全专家组成员；中国民生银行信息安全技术顾问。

长期从事信息安全的理论研究。
著有《网络安全技术概要》，《CPK标识认证》。

曾获国家科技进步二等奖、三等奖及军队科技进步一等奖、二等奖。

## 书籍目录

第1章 基本概念 1.1 物理世界和网际世界 1.2 无序世界和有序世界 1.3 有证书系统和无证书系统 1.4 基于标识的证明和基于第三方的证明 1.5 证明链和信任链 1.6 集中式管理和分散式管理 1.7 手写签名和数字签名 1.8 生物特征和逻辑特征第2章 鉴别逻辑 2.1 信任关系 2.2 相信逻辑 2.3 标识认证 2.4 可信逻辑第3章 组合公钥（CPK） 3.1 ECC密钥复合定理 3.2 标识密钥 3.3 密钥复合 3.4 数字签名 3.5 密钥交换 3.6 安全性分析第4章 体制的探讨 4.1 体制的需求 4.2 体制的发展 4.3 数字签名机制 4.4 密钥交换机制 4.5 信任根的讨论第5章 系统设计 5.1 认证网络 5.2 证书定义 5.3 数字签名协议 5.4 密钥交换协议 5.5 口令协议 5.6 数据加密协议 5.7 签名格式协议 5.8 证书生成协议 5.9 证书使用协议第6章 证书管理 6.1 密钥管理机构 6.2 行政管理第7章 CPK芯片 7.1 技术背景 7.2 主要技术 7.3具体实施方式第8章ID证书 8.1 技术背景 8.2主要技术 8.3具体实施方式第9章电子邮件认证 9.1 电子邮件的证书 9.2电子邮件作业过程第10章手机通信认证 10.1手机证书 10.2手机认证通信第11章 电子银行认证第12章 电子票据认证第13章 通信标签认证第14章 出入网关认证第15章 软件代码认证第16章 电子标签认证第17章 电子印章认证第18章 数字版权认证附件l：走出神秘的“ 黑屋 ”附件2：标识认证打开信息安全新天地附件3：CPK Cryptosystem附件4：我国解决世界难题的“ 电子身份证 ”引起国际关注附件5：CPK体制走向国际附件6：关于CPK若干问题的说明附件7：寻找安全“ 银弹 ”附件8：基于CPK体制的标识认证附件9：WebIBC：Identity Based Cryptography for Clinent Side Security in Web Applications参考文献后记：浅谈信息安全发展新动向

## 章节摘录

第1章　基本概念　　在认证理论的研究中，首先需要澄清一些基本概念。
随着互联网的发展，信息安全和网络安全得到了迅速发展，同时提出或产生了很多新的概念。
在新概念形成过程中难免不完善、不全面。
概念的不完善或不全面极容易引起误导。
如果这种误导影响到国家的决策，则会导致战略性错误。
因此，要把有争议的概念提出来，共同讨论、研究、澄清，以求共识。
1.1　物理世界和网际世界　　网际世界是IT技术发展的产物，称Cyber。
网际世界是新生事物，应该有它自己独特的发展规律，而只有把握了规律才能驾驭网际世界的发展。
这个规律的研究则刚刚起步，展示了广阔的研究前景。
认证体系首先在物理世界中产生，已经历了漫长的发展过程，形成了一整套法律、制度、技术、运行的机制。
网际世界是新近出现的新生事物，其认证体系的研究则刚刚起步。
到目前为止，物理世界还是大世界，而网际世界是小世界，是物理世界的一小部分。
然而网际世界在不断扩大，与物理世界越来越融为一体，构成更大空间的新的信息世界。

第一图书网, tushu007.com



## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com