

<<CPK标识认证>>

图书基本信息

书名：<<CPK标识认证>>

13位ISBN编号：9787118043105

10位ISBN编号：7118043109

出版时间：2006-10

出版时间：国防工业出版社

作者：南湘浩

页数：216

字数：181000

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>

<<CPK标识认证>>

内容概要

本书介绍了实现标识认证的CPK组合公钥算法。

CPK算法通过组合方法实现公私钥对的规模化，以很小的资源(如：60KB)，构造出规模很大的公钥(如10)空间；通过映射方法绑定标识和公钥。

本书介绍了以CPK bufft—in芯片实现的多标识域、多作用域的实名制认证系统，不再需要第三方证明和远程或外部设备的支持而当场验证，并且验证模块可以通用化、普及化。

本书以具体例子说明了CPK标识认证算法，在邮件地址、手机号码、账号、印章、IP地址、通信标签、软件标签、证件以及品名等标识认证中的应用。

标识认证是关系到在信息社会中建立秩序，构建可信系统的重大课题，将影响到可信交易、可信通信、可信计算、可信物流，并为实现信息世界的有效管理、垃圾邮件、以及网上取证提供有力的鉴别手段。

本书适合于从事信息安全的研究人员、开发人员、管理人员阅读，希望有助于树立新的安全观。

<<CPK标识认证>>

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。
曾获国家科技进步

<<CPK标识认证>>

书籍目录

第1章 基本概念 1.1 新一代安全 1.2 物理世界和网络世界 1.3 无序世界和有序世界 1.4 手写签名和数字签名 1.5 生物特征和逻辑特征 1.6 自身证明和第三方证明 1.7 对称密码和非对称密码 1.8 加密算法和鉴别算法 1.9 身份鉴别和标识鉴别 1.10 CA证书和ID证书 1.11 证书链和信任链 1.12 强制型和自主型策略 1.13 集中式管理和分散式管理 1.14 CPK和PKI认证系统第2章 认证系统的架构 2.1 概况 2.2 认证体系 2.3 认证网络 2.4 密钥管理第3章 密钥管理算法 3.1 IBE加密算法 3.2 ECC组合公钥算法 3.3 其他密钥组合算法第4章 ID证书 4.1 ID证书构成 4.2 证书体 4.3 变量体 4.4 证书组成形式第5章 认证协议 5.1 基于ID证书的主体鉴别协议 5.2 基于第三方的主体鉴别协议 5.3 数字签名协议 5.4 密钥交换协议 5.5 口令验证与更换协议 5.6 加密协议第6章 运行格式 6.1 格式定义 6.2 注释 6.3 运行特点第7章 电子办公认证系统 7.1 电子邮件认证系统 7.2 办公手机认证系统第8章 电子银行认证系统 8.1 电子银行证书 8.2 取款认证流程 8.3 转账认证流程 8.4 电子票据认证系统第9章 CSK算法的应用 9.1 客户证书 9.2 中心证书 9.3 qd心密钥矩阵的存储第10章 LPK算法的应用 10.1 改造PKI的必要性 10.2 改造PKI的可行性 10.3 具体实现方法第11章 行为的评分 11.1 鉴别行为树 11.2 主体鉴别与评分 11.3 客体鉴别与评分 11.4 行为鉴别与评分 11.5 评分汇总与信任体系的建立第12章 证书发行机制 12.1 密钥管理机构 12.2 行政管理第13章 美军CAC卡 13.1 标识管理的目标 13.2 CAC卡的内容 13.3 系统构成 13.4 CAC卡的发行过程 13.5 过去的ID卡和现在CAC卡的不同 13.6 CAC卡的启示第14章 CPK基础部件 14.1 CPK功能模块和协议模块 14.2 CPK ID证书第15章 CPK基础应用 15.1 CPK标签防伪 15.2 CPK可信计算 15.3 CPK可信连接 15.4 CPK认证网关 15.5 CPK数字版权 15.6 CPK电子印章第16章 基于CPK的标识认证 16.1 标识认证算法的形成 16.2 标识认证与网络秩序 16.3 标识认证与可信交易附件A PMT算法附件B ATM机的新旧兼容方案参考文献

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>