计算机终端信息安全保护系统

清华紫光股份有限公司

目录

公司简介

清华紫光股份有限公司是主营 IT 和通讯业务的 A 股上市公司（简称清华紫光，股票代码 000938）。公司股本结构中，清华大学控股 62%，社会流通股占 32%，其它国有法人股占 6%。

追根溯源，清华紫光有着 16 年的发展史。

1988 年，清华大学科技开发总公司成立，它是清华紫光的前身。

1993 年，清华大学科技开发总公司更名为清华紫光集团。

1999 年，清华紫光集团发起设立清华紫光股份有限公司。同年 8 月，清华紫光股票成功发行。

2000 年，清华紫光股票创下 106 元股价，成为中国股市百元股王。

2002 年，清华紫光集团并入新成立的清华控股有限公司，环保、药业分拆和资源重组，调整后的清华紫光股份有限公司成为专注信息产业方向的专营性公司。

目前，清华紫光股份有限公司下设 14 个事业部，控股 25 个公司，参股 28 个公司，业务领域广泛覆盖 IT 和通讯的主流方向。

清华紫光是国家 520 户重点企业、国家重点高新技术企业、国家 863 计划成果产业化基地、全国电子信息“ 百强 ”企业。曾荣获国家技术发明奖、北京市名牌产品等数十项奖励。

从 1988 年的 150 万元起家，经过 16 年的发展，清华紫光已达总资产 17 亿元，年产值 20 多亿元。

清华紫光集清华大学的特殊优势和 16 年的市场积累，以品牌、资源、资金为发展支点，以“ 简单、高效、健康“ 为管理思想，突出主营业务方向，并依此架构了三个业务群组：自有品牌产品群组、自有技术应用群组和渠道增值分销群组。公司力求以多样化的产品、系统化的技术应用和服务，多层次、持续性地满足消费者和用户的需求。

企业荣誉

国家 520 户重点企业
国家“ 863 ”计划成果产业化基地
全国电子信息“ 百强 ”企业
全国高新技术 “ 百强 ” 企业
国家科委评定的“ 实施火炬计划先进高新技术企业 ”
北京工业系统“ 双十佳 ”企业
北京市软件产业基地骨干企业
连续多年获北京市新技术开发试验区“ 经济二十强 ”企业
工商行、建行的“ 银企合作 ”企业
被科技部认定为“ 国家重点高新技术企业 ”

产品荣誉

国家技术发明奖
国家科技进步奖
国家重大技术装备成果奖
国家级火炬计划项目
国家级重点新产品
国家级科技成果重点推广计划项目
国家教委科技进步奖
北京市科技进步奖和北京市名牌产品
北京新技术产业开发试验区拳头产品
北京市重大科技成果推广计划

海淀试验区十大名优品牌产品
联合国中国分部发明创新科技之星
中国优秀软件产品

业务资质

计算机信息系统集成壹级资质
涉及国家秘密的计算机信息系统集成资质
公路交通工程专业承包通信、监控、收费综合系统工程资质
电子工程专业承包贰级资质
建筑智能化专项工程设计甲级资质
建筑智能化工程专业承包贰级资质
ISO9001 质量管理体系合格证书
AAA 信用等级证书

项目简介

一、项目目的：

开发基于智能卡的计算机安全防护系统，给计算机增加硬件身份认证和硬件文件加密功能，防止计算机中的重要信息被非法浏览、窃取、篡改、破坏或删除，即使计算机丢失或被盗，也能防止信息泄漏，全方位对计算机内的各种文档资料实施保护。

二、项目意义：

随着我国信息化建设的蓬勃发展，国民经济和社会发展对信息系统的依赖性越来越强。由于现有的通用计算机根本就没有安全防护措施，就象一个门窗大开的屋子，任何可以接触计算机的人都可以访问其中的信息，加之社会发展的不稳定因素，使得重大信息安全事件连连发生，不仅直接影响到国民经济的正常运行，给国家造成巨大的经济损失，而且也危及我国政治、军事、经济、文化、社会生活的各个方面，危及国家的安全和社会的稳定。

当今世界的冲突已经从物质资源和能源资源的争夺演变为信息资源的争夺，信息安全已成为维护国家安全和社会稳定的一个焦点。2003 年 7 月 22 日召开的国家第三次信息化领导小组会议上，中共中央政治局常委、国务院总理、国家信息化领导小组组长温家宝主持会议并作重要讲话，温家宝总理明确指出“ 信息安全已经成为国家安全的重要组成部分 ”，会议讨论通过了《关于加强信息安全保障工作的意见》（中办发［2003］27 号）。《意见》中特别提到了加强信息安全技术研究开发，推进信息安全产业的发展，显而易见，保证国家信息安全工作已经成为国家的当务之急。

为了落实贯彻《意见》精神，国务院于 2004 年 1 月 9 日在北京召开了全国信息安全保障工作会议。中共中央政治局常委、国务院副总理黄菊出席会议并作重要讲话。他说，必须充分认识做好信息安全保障工作的极端重要性，全面提高信息安全防护能力。

三、项目必要性：

提起信息安全，人们自然就会想到黑客攻击和病毒破坏，认为只要部署了防火墙、入侵检测系统、防毒杀毒系统就安全了。但是美国联邦调查局（FBI）和计算机安全机构（CSI）的调查结果表明：超过 80%的信息安全隐患来自内部，而非外来黑客和病毒引起，信息泄露所造成的损失是被病毒破坏的 18 倍，是被黑客攻击所造成损失的 36 倍。

中国国家信息安全测评认证中心提供的调查结果也显示，信息安全问题在很多情况下都是由“ 内部人士 ”所为，而非外来黑客和病毒引起。国家信息化专家咨询委员会委员沈昌祥教授在 2003 年中国信息安全技术大会上对我国信息安全系统和产业进行了反思：“ 世界上相关统计表明，信息安全的攻击 75%以上是内外勾结所造成的，这种趋势还在逐步上升，我国的信息安全假设不对头，我们花的钱是解决 15%的问题、25%的问题，还是解决 75%的问题？一定是这 75%的问题。信息想要安全，首先要对使用者进行控制和管理，要进行信息的访问控制 ”。

计算机的开放性、易用性和标准化等特点，使计算机信息具有共享和易于扩散的特性，导致计算机信息始终面临着泄露、窃取、篡改和破坏的巨大危险。如何保护现有计算机中的关键信息不被非法获取、盗用、篡改和破坏，已成为当前我国信息安全保障工作中急待解决的问题。

1.1. 四、本领域国内外研究开发现状和发展趋势

为了保证计算机数据库、数据文件和所有数据信息免遭泄露、窃取、更改或破坏，通常采用身份识别技术和数据加密技术对计算机数据信息进行保护。

身份认证的主要目的是鉴别用户身份，区别合法用户和非授权用户，防止攻击者假冒合法用户获取访问权限，强有力的身份认证技术能够在计算机周围构筑一个安全屏障。 现有的计算机大多使用口令密码方式进行身份认证。这种方法的安全性仅取决于用户口令的保密性，口令密码很容易被泄漏、忘记或破译，不能抵御口令猜测攻击。

解决上述问题的有效方法是采用智能卡（Smart Card）进行身份认证。智能卡也称 IC 卡，具有很高的安全保密性，而且不易伪造。智能卡中的操作系统可防止攻击者利用软件方式窃取智能卡内的机密信息。智能卡从芯片制造到封装采用了一系列安全措施，可以抵御物理、电子、化学方法的攻击。

加密技术是保障数据安全的最有效和最可靠方法。将信息（明文）经过密钥和加密算法，转换成很难识别的密文后进行存储和传输，即使中途被截获，也无法理解信息内容，可以保证只有被授权的人才能阅读该信息，从而避免信息泄漏。加密技术的安全性取决于密钥的安全性，加密算法可以公开，只要密钥不被泄露，则无法破解密文。

密钥应存储在不可访问的安全载体上，而且还要加密保护，防止非法用户用软件方式盗取、篡改和复制密钥。而计算机中现有的各种存储器，如硬盘、软盘、光盘和 U 盘均无法满足密钥存储的要求。使用软件进行数据加密时，操作系统会将加密程序和密钥写在硬盘上，攻击者很容易在硬盘上搜索到加密程序和密钥，因此软件加密技术的安全性很低，容易破解。

解决计算机数据安全问题的根本出路，是给计算机增加一个独立的硬件安全子系统，建立一个安全封闭的计算环境，对重要信息进行加密处理，同时阻止非法用户的访问和破坏，从硬件层面上彻底解决计算机信息安全问题。

在一些重要部门，均采用专用的加密卡或加密机对计算机数据进行加密，并配合智能卡进行身份认证。由于计算机内安装加密卡等硬件可大大提高系统安全性，但它们价格昂贵，安装、使用不方便，目前只限于小范围内的应用，没有得到普及。

IBM 和微软分别在 2002 年和 2003 年推出了计算机数据安全问题解决方案， IBM 和微软都将以安全芯片为核心的安全子系统嵌入到计算机主板上，与相应的安全软件（提供操作系统、应用软件与安全芯片之间的接口）结合使用，克服了通用计算机数据可被轻易读取的缺陷，提供了前所未有的安全防护性能。IBM 和微软都希望各自的安全芯片和核心软件将来会成为计算机的标准配置，进而达到垄断计算机数据安全防护市场的目的。

由于智能卡本身就是一种安全子系统，具有身份认证、加密、解密、签名和鉴别等多种安全保密手段，因此国外很多公司都纷纷开展了将智能卡用于计算机身份认证和数据加密的应用开发工作，并将智能卡与 USB 接口集成于一体，不需要智能卡读卡器，只需将带有 USB 接口的智能卡插入计算机 USB 接口，就可给计算机增加信息安全防护系统，使计算机具有硬件身份认证和硬件数据加密功能。安全性是计算机未来发展的主旋律，下一轮计算机的升级换代将不仅仅是 CPU 速度提高和操作系统升级，更重要的是信息安全等级的提高。

一、产品概述

计算机终端信息安全保护系统是一种基于硬件身份认证方式的桌面数据安全保护系统，保护计算机系统及重要文件（如政府文件、商业机密和个人隐私等）不被非法窃取、非法浏览的计算机信息安全产品。防止计算机中的重要信息被故意的或偶然的非授权用户偷窥、窃取、泄漏、更改、破坏或删除，全方位保护信息安全。

计算机终端信息安全保护系统可以控制 Windows 系统登陆，可以控制电脑 USB 接口和网络端口，可将电脑中的任意一个文件夹设置成“ 保险箱 ”(可设置多个)，只有在 USB 接口插入 S 锁，并输入正确的密码后才能打开保险箱。这个文件“ 保险箱 ”实际是一个隐形的文件夹，只有保险箱的建立者才可使用它，这个隐形文件夹对合法使用者是透明的，你可以用 WINDOWS 方式对它进行读、写等操作，进入保险箱的文件或目录被自动加密，离开保险箱的文件或目录被自动解密。一旦安装了本系统，专用的 S 锁就成为开启您电脑中信息保险箱、进入 Windows 系统、使用 USB 接口等设备的唯一合法手段，本产品具有软硬件双重保护作用。

只有在 USB 接口插入 S 锁，并输入正确的密码后才能打开保险箱、打开 USB 接口、网络端口等。

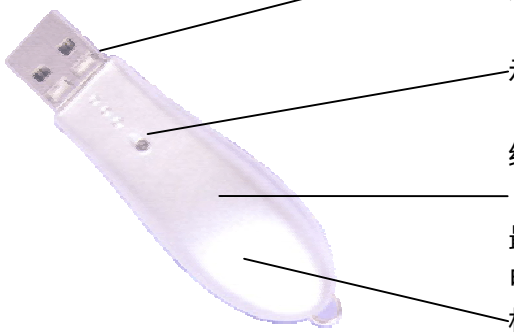
如果没有 S 锁，即使密码被人窃取，别人也无法冒充身份打开保险箱。只有合法用户进入保险箱后，才可以在其中创建目录，浏览和存放需要保护的重要文件和数据。

从 USB 接口拔出钥匙后，文件保险箱及保存在保险箱中的所有文件和数据都自动从系统资源界面中消失，即使有高手能够将它们从硬盘中挖掘出来，所有内容也都是乱码，即使非法使用者将硬盘从电脑中取出，安装在其他电脑中，仍然无法读取数据，保证重要资料不被泄露。

还可利用密码钥匙和口令锁定计算机，只要拔出密码钥匙，计算机自动锁定键盘、鼠标、屏幕等外部设备，防止非法用户恶意操作计算机，对重要数据进行偷看、篡改或删除。

二、规格参数

2．1 产品性能



使用 USB 接口通讯，符合 USB1.1 技术规范，通讯速率 1.5Mb/s

具有一个 LED,用于电源指示和通讯指示

内置智能卡，具有 SmartCOSPK 操作系统的所有功能

用户存储空间为 16K

最大功耗：100mW

电源 5V，由 USB 接口直接供给

相对湿度:30%~95%

- S 锁 = 明华 USB 读写器 + SmartCOS PK 智能卡
- 可热插拔达 10 万次以上，抗震性强，防潮，防磁，耐高低温
- 标准的USB 接口、即插即用、无设置及硬件冲突之忧，适用于PC机、笔记本电脑、服务器及其他网络设备的USB接口，通讯速率1.5Mbps
- 内置 CPU 智能芯片、具有 SmartCOS PK 操作系统的所有功能，数据存于芯片中，极为安全可靠
- 用户存储空间为16K用以存储个人信息、密码、密钥、证书等
- 密钥存于紫光S锁 中，运算也在紫光S锁 中完成，无法跟踪
- 支持DES、3DES 密码算法及国家密码管理委员会办公室批准的专用的分组密码算法
- 支持RSA1024bit、ECC160bit/192bit 公钥算法
- 直接在芯片内快速生成RSA 或ECC 密钥对，可实现签名/认证、加密/解密功能
- 支持MD5、SHA-1 数据散列算法
- 内置硬件随机数发生器
- 适用于 WINDOWS98/ME/NT/2000/XP 及 Linux 等系统

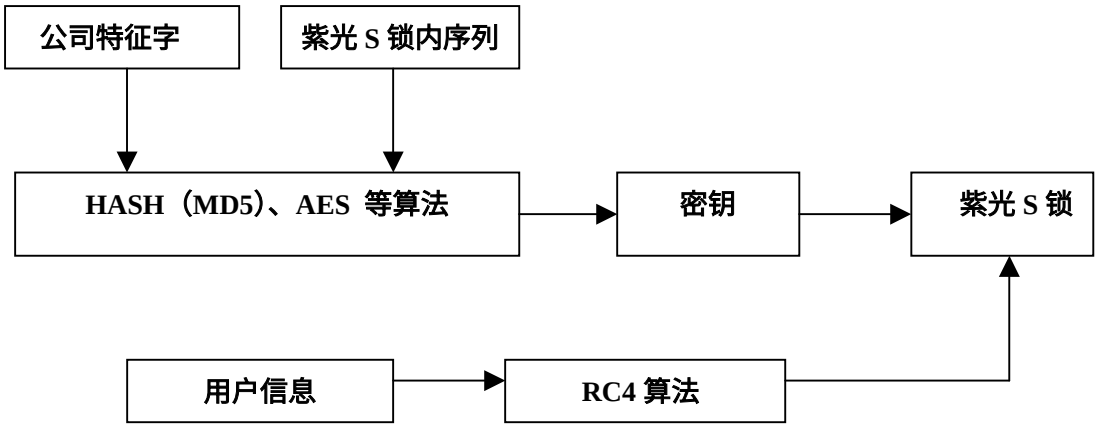
2．2 产品特性

- 128 位存贮单元 12mhz 处理器
- 中间件(Middleware)：PKCS#11，微软 CSP
- 符合 X.509V3 数字证书存储标准
- 软件控制状态指示灯
- **64 位全球唯一系列号**
- 口令保护，防止文件被读取/修改

三、身份认证的方案及流程图

3．1 证书及密钥的生成：

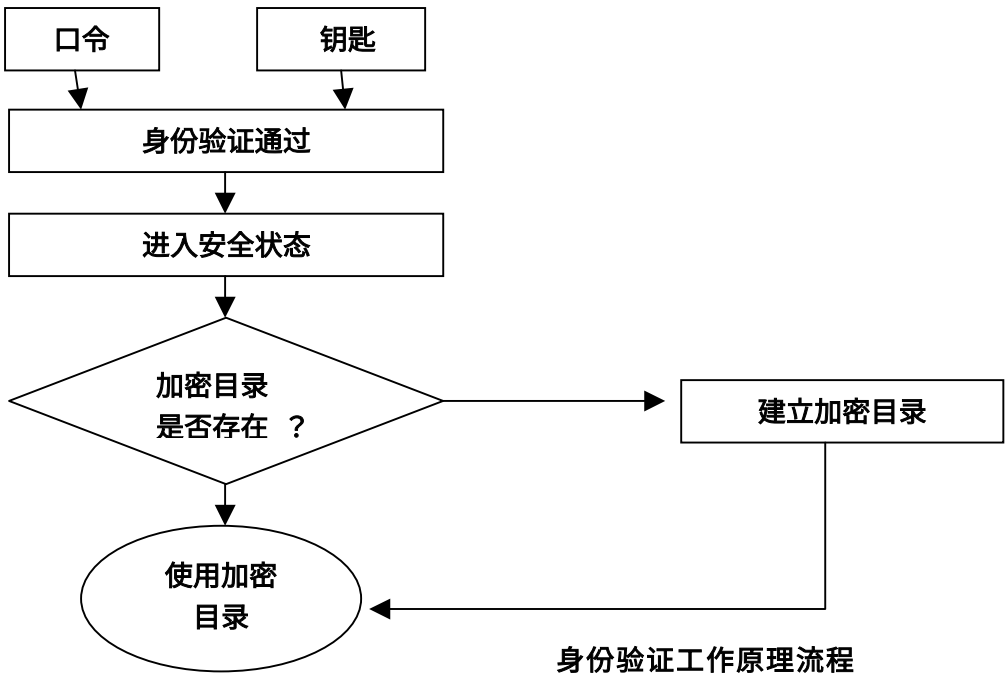
由证书生成程序向紫光 S 锁内写入用户信息和用户加密/解密密钥，具体方法是用紫光 S 锁内唯一的产品序列号作为种子，产生 128 位的用户加密/解密密钥，使得每把硬件钥匙内的数字密钥具有唯一性，密钥重复出现的可能性为 $1/10^{38}$。



证书生成工作原理流程图

3．2 身份验证

采用口令和硬件双重身份认证，必须插入硬件钥匙并输入相对应的口令才能通过身份验证，之后，为防止非法进入系统，连续三次输错口令，系统将自动关闭身份验证窗口。

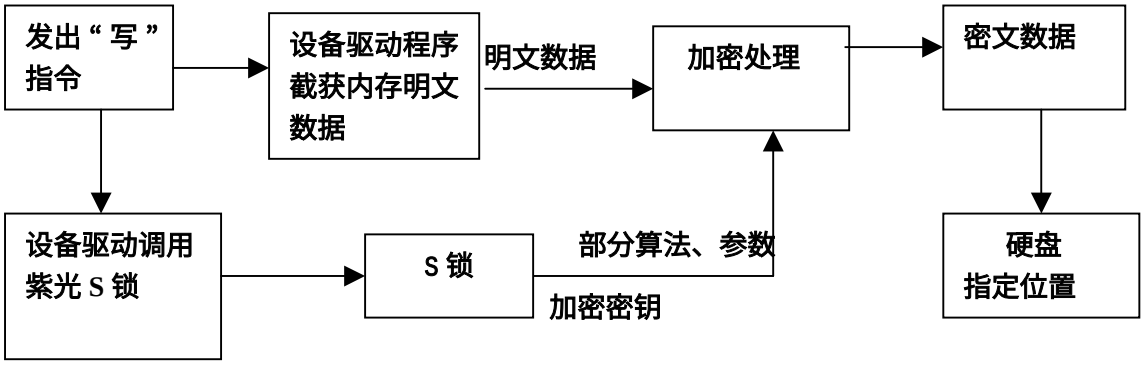


身份验证工作原理流程

四、文件加/解密

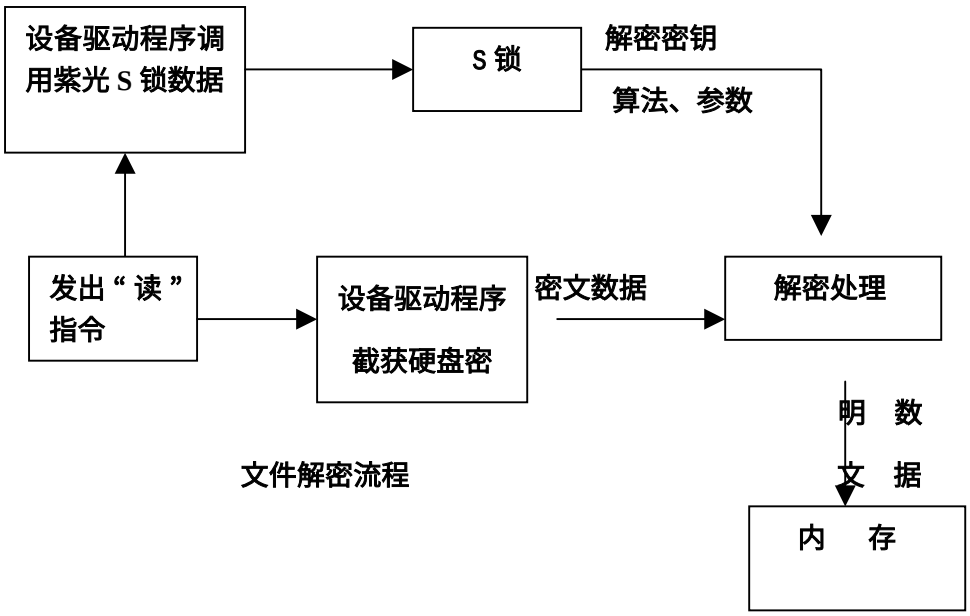
4．1 文件加密：

当操作系统对文件发出“写”指令时，(WINDOWS 操作系统提供的对文件存储、拷贝粘贴、拖动等功能）由设备驱动程序截获内存中明文文件的数据流，同时调用紫光 S 锁中的加密密钥及部分加密算法和加密参数，将明文数据加密后存入指定的硬盘加密空间。



4．2 文件解密

当操作系统对文件发出“读”指令时，(WINDOWS 提供的对文件打开、拷贝粘贴、拖动等功能）硬盘加密文件的数据流被设备驱动程序截获，同时设备驱动程序调用紫光 S 锁中的解密密钥和部分算法及参数，经解密后还原成明文数据置内存。



文件解密流程

五、计算机开发系统锁定技术

（略）

六、安全功能：

1、防非法用户

双重身份保护。只有将密码钥匙插入计算机 USB 接口中，并输入正确口令后，“ 保险箱 ”才能显现在系统资源界面中。

如果拔出密码钥匙:

①文件保险箱及保存在保险箱中的所有文件和数据都自动从系统资源界面中隐藏;

②计算机自动锁定键盘、鼠标、屏幕等外部设备，防止非法用户恶意操作计算机，对重要数据进行偷看、篡改或删除，保证数据安全。

2、防止因丢失笔记本电脑或硬盘而泄密

基于硬件加密技术的信息保险箱,不仅能被隐藏，更重要的是能对保险箱中的内容加密，加密的密钥在硬件钥匙中，他人无法通过穷举程序或黑客程序获得你的加密密钥，只要硬件钥匙不丢失，即使窃取了你的口令，也无法对加密文件进行解密。因此：

①即使非法使用者将硬盘从电脑中取出，安装在其他电脑上；

②或窃走你的笔记本电脑;

仍然无法读取你保险箱中的数据，保证重要资料不被泄露。

3、防止非法传输/拷贝

传统的电脑是完全开发的系统结构，紫光 S 锁通过控制 USB 接口、网络通讯端口、软驱、光驱等设备以及电子邮件、FTP 等传输协议防止非法拷贝和传输数据。

4、防止网上邻居通过共享而窃密

如果你的“保险箱”所在的逻辑硬盘是共享的，合法使用者正在使用保险箱中的文件，此时，保险箱中的密文在内存中已转为明文，但是，网上邻居无法通过共享浏览到你正在打开的内存中的明文。

5、防止突发事件造成的泄密

有时，计算机在操作时会发生死机或突然断电，这时 WORD 文件系统会自动产生一个临时文件保留在当前目录下，紫光 S 锁会自动将其加密，保证在任何情况下“保险箱”中的文件始终是密文。

七、技术特点：

1、口令和硬件双重身份认证

采用口令和硬件双重身份认证，必须插入硬件-紫光 S 锁并输入相对应的口令后才能通过身份验证，解决了传统密码认证方式密码容易被泄漏、忘记、破译的缺陷。为防止非法进入系统，连续三次输错口令，系统将自动关闭身份验证窗口。

2、算法

采用国家密码委批准的 F33 算法，将文件加密密钥由 F33 算法加密后存放在硬件中。文件的加密/解密过程必须从硬件中将密钥解密后方可完成文件的加/解密。

硬件中含有公私钥体制长度为 1024 位的 RSA 算法，随机函数产生一次一密的加密密钥，支持基于软硬件的网络双向身份认证系统的应用。

支持第三方加密算法可同第三方算法无逢连接。

2、硬件加密技术

加密钥匙不同于软件狗，藏于软件狗内的密码容易破译，而加密钥匙采用智能卡技术，钥匙内含 CPU，加密密钥和加密参数被固化在钥匙中，加密密钥的生成和保存全部在钥匙芯片内部进行，不进入计算机环境，完全杜绝黑客程序的跟踪和攻击。他人无法获取和复制，窃密者无法通过软件破译算法密钥进行解密。

3、安全芯片操作系统

本产品 USB 紫光 S 锁使用通过中国人民银行认证的 SmartCOS 安全芯片操作系统，有效防止 USB 安全钥匙中的数据被非法窃取或篡改，使非法用户无法复制或伪造 USB 安全钥匙。

4、动态加密技术

这是本产品最具特色的加密技术。她将要加密的数据在写入保密文件夹时动态加密处理，将要解密的数据在读取时动态解密。因此，保证在任何情况下磁盘文件始终是密文，例如 Word 产生的临时文件、以及突然断电或死机时应用程序留在电脑中的临时文件都是加密的密文，即使是从加密目录中删除到垃圾站的文件仍然是密文。

5、操作系统无缝链接

可像操作普通文件一样，将重要的文件拖放、拷贝、粘贴到信息保险箱内，系统自动完成对文件的加密处理；同样，可像操作普通文件一样，将重要文件从保险箱内拖放、拷贝、粘贴到保险箱外，系统自动完成对文件的解密处理。

6、支持声纹/指纹识别的身份验证

可将口令验证改为声纹/指纹验证，用声纹/指纹代替口令密码，使验证方式更具人性化和个性化。

7、用于身份识别的敏感信息具有高可靠性

在产生证书时将用户信息、时间函数等通过 RC4 等算法加密后写入安全钥匙-紫光 S 锁中，验证身份时需要从硬件中读取数据，每把紫光 S 锁的身份识别数据不可复制、不可重复。

8、加密密钥的产生

用固化在安全钥匙—紫光 S 锁中的 64 位全球唯一序列号做种子，经 HASH 等算法运算产生加密密钥，加密密钥存放在硬件中；由硬件特性决定了密钥的不可复制性和不可重复性。

9、密钥的管理

产品在出厂时已由生产方将用户身份识别信息和加密密钥写入硬件中，同时，系统发证机关详细记录了每把钥匙的原始信息，如果合法人不慎将安全钥匙丢失或损坏，其保险箱内的加密数据将无法恢复成明文，为了保证意外情况发生时合法人的重要文件不丢失，系统的发证机关提供恢复证书和密钥的功能，该功能将依据保修卡上的产品序列号，从证书库中提取对应的原始信息，重新生成一把新钥匙。

如果钥匙保存完好而忘记口令的情况发生，也无法再从保险箱中读取数据，系统将用上述同样方法，将原始信息重新写入钥匙，恢复钥匙中的原始口令密码，即可恢复保险箱中的密文。

10、密钥和证书的安全性

对于特殊的安全级别高的应用群体，比如重要的机关、部队等，如要求由自己产生和保留证书及密钥的信息，系统可提供独立的发证机关，由使用者自己产生、发放证书。

八、产品特性

1、简单易用：

进入保险箱就像“用钥匙打开家门一样方便”。将紫光 S 锁插入 USB 接口，并输入正确口令后，即可实现用户身份认证，并打开保险箱。用鼠标将文件拖入/出保险箱，紫光 S 锁自动对文件进行加/解密运算。拔出紫光 S 锁后，系统立即被锁定。

2、安全性高：

口令和硬件双重身份认证，自动对放入文件保险箱的文件进行查毒和杀毒，加密密钥以密文形式存放在 USB 安全钥匙内，部分算法参数也存放在钥匙内，非法用户破译计算机硬盘中的密文难度极大。

3、透明操作：

与 Windows 操作系统无缝链接，可像操作普通文件一样，将重要的文件拖放、拷贝、粘贴到“文件保险箱”内。

4、兼容性强：

兼容 Window 98/2000/ME/NT/XP 等主流操作系统。

5、高可靠性：

采用高科技材料，可热插拔达 10 万次以上，抗震性强，防潮，防磁，耐高低温，抗静电干扰。

九、测试报告

各项内容通过公安部计算机信息系统安全产品质量监督检验中心和中国人民解放军信息安全产品检测中心检测通过。

9．1 测试环境

局域网内计算机、独立的笔记本

9．2 测试平台

测试平台：WINDOWS98 所有版本、WINDOWS ME、WINDOWS 2000 Professional、WINDOWS XP Professional。

9．3 测试内容

各类文件的加密和解密

、文本类文件（.txt,.doc,.rtf,.wri,.htt,.htm,.html,.ppt,.nfo,.xls,.pdf） 2、应用程序类文件（.exe,.com） 3、图象类文件（.bmp,.jpg,.gif,） 4、音频类文件（.mp3,.wav,） 5、压缩类文件（.cab,.zip,.rar） 6、视频类文件（.dat,.mpg,.avi）	在加密文件夹内和在加密文件夹外 1、可以进行编辑（修改文本、图象等信息）。 2、可以进行文件以及文件夹的操作（复制、剪切、粘贴）。 3、可以进行文件以及文件夹的同盘和异盘操作。 4、可以在加密目录内外进行新建、保存、另存为操作。 5、可以正常设置文件的属性。 6、正常和非正常重启、关机工作正常。 7、加密文件及文件夹大小没有限制。 8、可以防止加密目录在正常和非正常共享后，不被其它计算机看到。	1、新建： 1．在加密目录下右击鼠标右键，新建一个文件、文件夹。 2．先打开程序，然后存在加密目录下。 2、保存：(在加密目录下) 1．直接打开文件，然后选择保存。 2．直接打开文件，修改后选择保存。 3．直接打开文件，关闭窗口时保存。 4．直接打开文件，修改后选择保存。 3、另存为： 1．打开程序，输入内容后，另存为到加密目录下。 2．直接在加密目录外，打开文件，另存为到加密目录内。 3．在加密目录内打开文件，另存为到加密目录内。 4、同盘（同一个驱动器）操作和异盘符操作： 1．将没有加密目录的盘上文件复制，粘贴到加密目录内。 2．将加密目录内的文件复制，粘贴到加密目录内。 3．将没有加密目录的盘上文件拖拽到加密目录内。 5、文件属性(隐藏、只读、压缩、加密)： 1．在加密目录外，对文件、文件夹选上隐藏属性，然后拖拽到加密目录内。 2．在加密目录内，对文件、文件夹选上隐藏属性，然后拖拽到加密目录外。 3．在加密目录外，对文件、文件夹选上只读属性，然后拖拽到加密目录内。	1、正常（和没有安装本软件时，WINDOWS 操作系统下的新建、保存、另存为操作后打开的结果相同） 2、各种文件类型工作正常。 3、加密目录即使在共享时，也不被另一台计算机所访问。 4、设置文件及文件夹属性（隐藏、只读、压缩）时工作正常。 5、与 WINDOWS2000 和 WINDDOWSXP 的加密功能不相容。 6、加密文件及文件夹大小没有限制。 7、正常和非正常的重新启动计算机和关闭计算机对加密文件没有影响。

		4．在加密目录内，对文件、文件夹选上只读属性，然后拖拽到加密目录外。 5．在加密目录外，对文件、文件夹选上压缩属性，然后拖拽到加密目录内。 6．在加密目录内，对文件、文件夹选上压缩属性，然后拖拽到加密目录外。 7．在加密目录外，对文件、文件夹选上隐藏和只读两个属性时，拖拽到加密目录内。 8．在加密目录内，对文件、文件夹选上隐藏和只读两个属性时，拖拽到加密目录外。 9．在加密目录外，对文件、文件夹选上加密属性，拖拽到加密目录内。 10．在加密目录内，对文件、文件夹选上加密属性，拖拽到加密目录外。 6、 重新启动、注销、关机： 1．在加密目录下，创建一测试文件（任意格式），注销当前用户。 2．在加密目录下，创建一测试文件（任意格式），重新启动计算机。 3．在加密目录下，创建一测试文件（任意格式），关闭计算机。等待十几秒后打开。 4．在加密目录下，创建一测试文件（任意格式），直接热重启。 5．在加密目录下，创建一测试文件（任意格式），直接冷重启。 7、 加密文件大小 1．单个文件或文件夹拖入加密目录。 2．十兆文件及文件夹拖	

		入加密目录。 3．两百兆文件及文件夹拖入加密目录。 4．六百兆文件及文件夹拖入加密目录。 5．一千二百兆文件及文件夹拖入加密目录。 8、用冰河木马感染被测计算机，从局域网计算机上控制，查找加密目录。	

十、同类产品比较和分析

目前应用于个人计算机文件加密的产品可分为以下三种类型

1、 纯软件：优点：价格便宜也有免费下载的，30 元左右的，能对本地硬盘文件加密；

缺点：算法简单，安全度低，容易破译，使用复杂，不易掌握和操作、非计算机专业人员更难使用。

2、加密 U 盘：(一般用户很容易将“ S 锁 ”同加密 U 盘混淆)

优点： 价格便宜（根据存储量不同，价格在 200—500 元之间)， 硬件本身既能存储文件又能将所存文件加密；

缺点： 只能加密 U 盘，不能对计算机本地硬盘加密，加密机制和算法简单，一般采用口令加密，易于攻击，安全强度差。

以上两种产品无论从技术、安全构架、安全强度、和国家政策法规上都无法同紫光 S 锁相比，紫光 S 锁采用专用加密钥匙，钥匙内含 CPU，含国家密码委批准的标准算法，含 RSA 公私钥体制，操作系统和认证数据通过硬掩膜写入硬件，是当前个人计算机文件保密最可靠的产品。

市场加密产品对照表

产品名称	**功能**	**操作方法**	**算法**	**硬件保护**	**合法资质**	**安全强度**	**计算机发生故障时,对加密文件的保护**
加密软件	文件加密	复杂	简单	无	无	个人防护级	易泄漏
加密 U 盘	文件加密	较复杂	口令	无	无	个人防护级	易泄漏
加密钥匙（其他品牌）	①文件加密 ②屏幕保护 ③计算机锁定	一般	简单	有	公安部认证	企业防护级	易泄漏
紫光 S 锁	①文件加密 ②文件隐藏 ③屏幕保护 ④计算机锁定 锁定 USB 接口	透明操作	标准算法	有	①公安部认证 ②密码委认证 ③中国人民解放军 军 C+	专业防护级	不泄漏

产品资质

一、公安部《计算机信息安全产品检验报告》

报告编号：公计检 030090

检验报告

样品名称	紫光计算机信息安全保护系统（紫光S锁）
型号规格	Ver 2.0
受检单位	清华紫光股份有限公司
检验类别	委托检验

公安部计算机信息系统安全产品质量监督检验中心

《检验报告》第二页

公安部计算机信息系统安全产品质量监督检验中心

检 验 报 告

共 4 页 第 2 页

检测设备：

1. 硬件设备
   PC机 二台
   网络附件若干

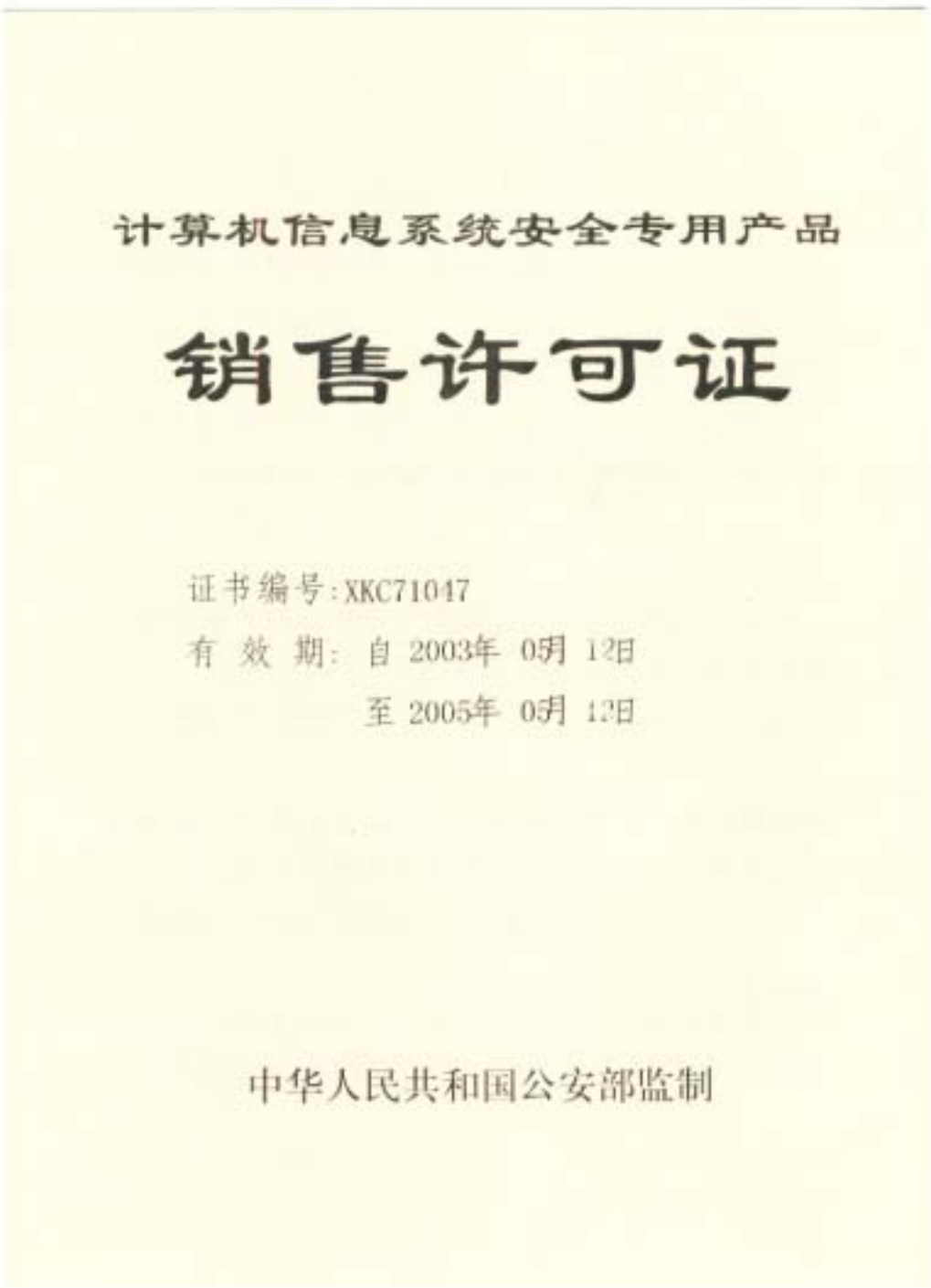
2. 软件设备
   操作系统
   Windows 2000 Server
   Windows 2000 Professional

3. 网络环境
   由产品和PC机组成的基于TCP/IP的网络测试环境。

产品概述：

由清华紫光股份有限公司送检的紫光计算机信息安全保护系统（紫光S锁）Ver 2.0，是对文件进行加密并保护的软、硬件结合的产品。该产品使用深圳明华澳汉科技股份有限公司的SZD12智能密码钥匙（eKey，USB接口）。

二、公安部《计算机信息系统安全专用产品销售许可证》



计算机信息系统安全专用产品

销售许可证

证书编号:XKC71047

有 效 期: 自 2003年 05月 12日

至 2005年 05月 12日

中华人民共和国公安部监制

清华紫光股份有限公司：

根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产的（代理）紫光计算机信息安全保护系统(紫光S锁) Ver2.0 ——

——————————————————————

——————————————————————安全专用产品进入市场销售，特发此证。

2002年 05月 12日

三、中国人民解放军《军用信息安全产品认证证书》军 C+

军用信息安全产品

认证证书

军密认字第 0206 号

产品名称：计算机信息安全保护系统（紫光 S 锁）TH-UC

研制单位：清华紫光股份有限公司

认证等级：军 C+（试行）

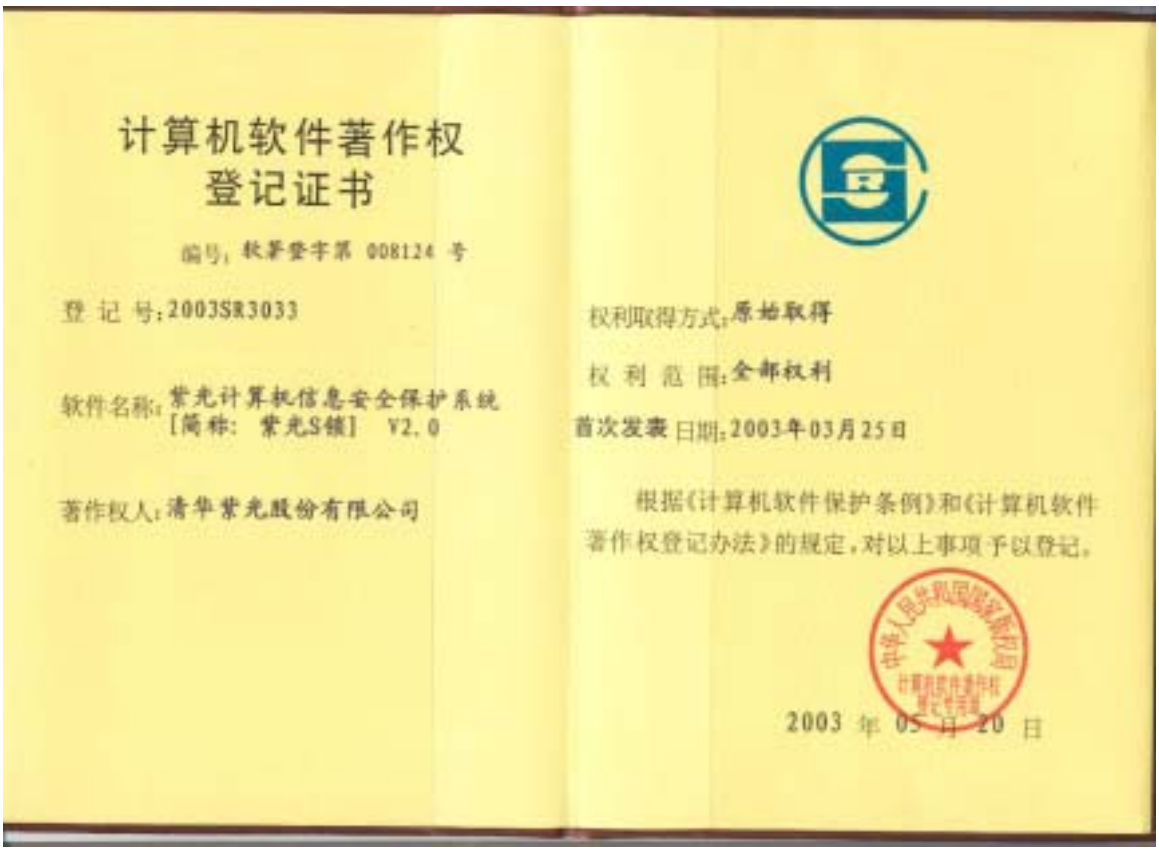
有 效 期：2003 年 9 月至 2005 年 9 月

中国人民解放军

信息安全测评认证中心

2003 年 9 月 8 日

四、国家版权局《计算机软件著作权登记证书》



计算机软件著作权
登记证书

编号：软著登字第 008124 号

登 记 号：2003SR3033

软件名称：紫光计算机信息安全保护系统
[简称：紫光S盾] V2.0

著作权人：清华紫光股份有限公司

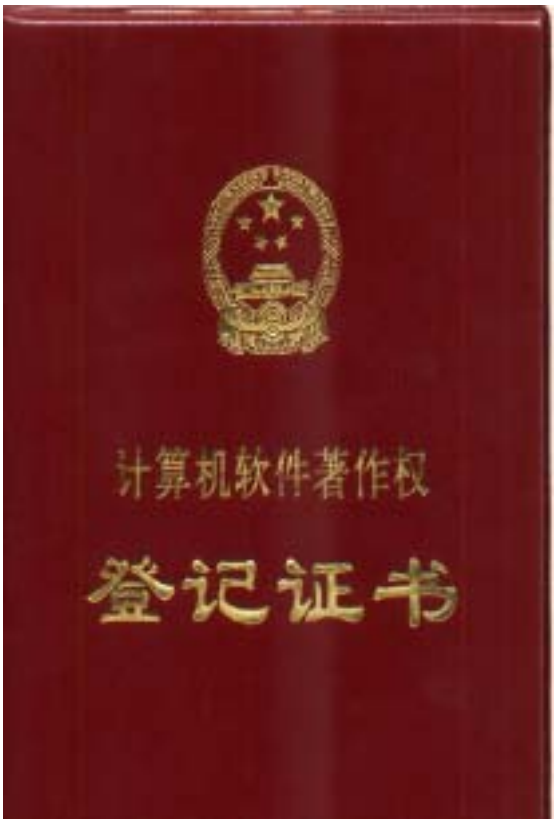
权利取得方式：原始取得

权 利 范 围：全部权利

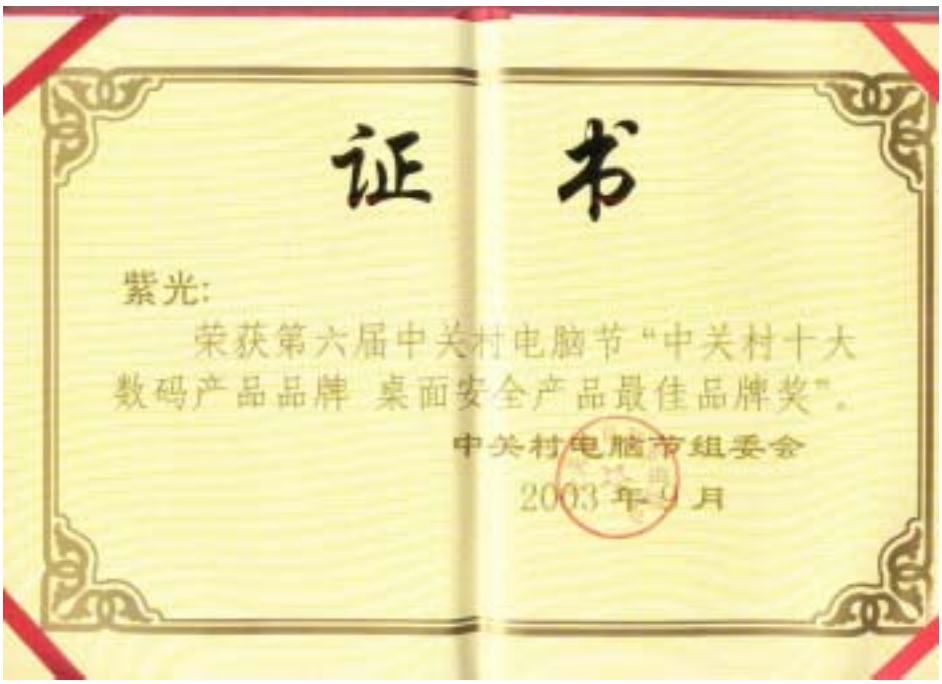
首次发表日期：2003年03月25日

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，对以上事项予以登记。

2003 年 05 月 20 日



五、中关村电脑节“ 桌面安全产品最佳品牌奖 ”


证 书

紫光:

荣获第六届中关村电脑节“中关村十大数码产品品牌 桌面安全产品最佳品牌奖”。

中关村电脑节组委会

2003年9月

六、国家保密局《涉及国家秘密的计算机信息系统集成资质证书》

涉及国家秘密的计算机信息系统集成

资质证书

编号：

经审查，核定 清华紫光股份有限公司

为涉及国家秘密的计算机信息系统集成单位，特发此证。

证书有效期：三年

发证机关

七、国家密码管理委员会《商用密码产品技术坚定证书》

商用密码产品
技术鉴定证书

证号：国密证第 0095号

深圳市明华澳汉科技股份有限公司：

你单位研制的 SZD12 智 能
密码钥匙 已通过国家密码管理
委员会办公室组织的技术鉴定。

特发此证。

国家密码管理委员会办公室
2001年12月19日

说明：

清华紫光 S 锁硬件采用深圳明华的电子智能钥匙——SZD12 智能密码钥匙，该公司是国家商用密码产品定点生产单位，该智能密码钥匙通过国家密码委员会技术鉴定，完全符合国家密码产品有关技术要求和标准。其他任何非国家定点生产单位不得生产密码产品。

八、合作伙伴资质证明：

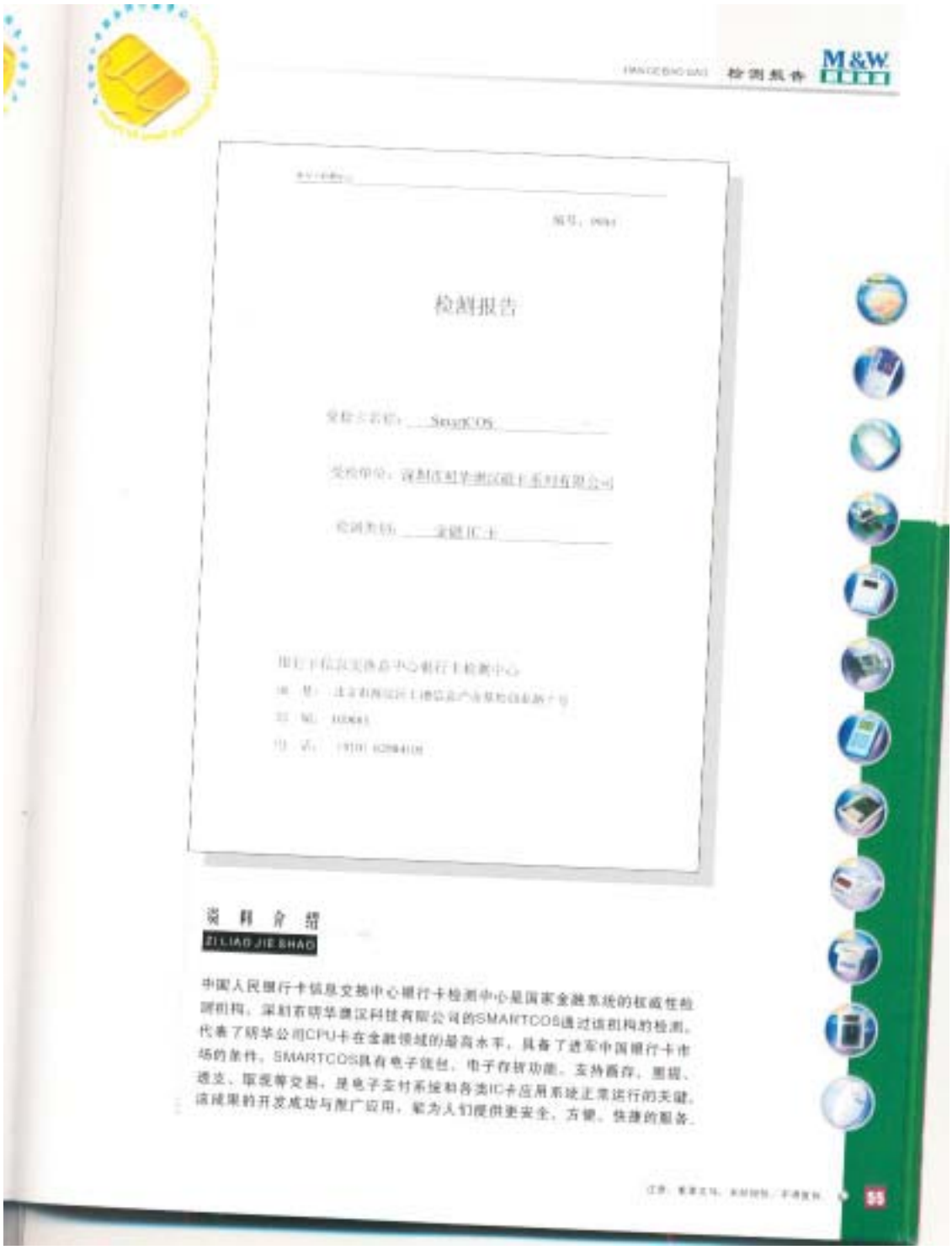
1、国家密码管理委员会办公室（通知）《商用密码产品生产定点单位的通知》

国家密码管理委员会办公室(通知)

关于批准深圳市明华澳汉
科技有限公司为商用密码产品
生产定点单位的通知

2、国家密码管理委员会办公室（通知）《关于同意研制 SZD12 智能密码钥匙》

3、中国人民银行银行卡信息交换中心产品检测（SmartCOS）



说明：

清华紫光 S 锁硬件采用深圳明华的电子智能钥匙，其内部的 SmartCOS 通过中国人民银行银行卡信息交换中心产品检测，符合《中国集成电路（IC）卡规范》，说明可以作为电子钱包、电子存折等载体使用，性能稳定、安全、加密强度高等特点。

后记：

人类已经进入了信息时代，信息无处不在，保护信息安全是国家、单位、个人都应该重视的。计算机信息安全问题解决不好，不仅会造成巨大的经济损失，甚至会危及国家的安全和社会的稳定。调查显示，超过 80%的信息安全隐患来自内部，信息泄露事件占所有信息安全事件的 30%~40%，信息泄露所造成的损失是被病毒破坏的 18 倍，是被黑客攻击所造成损失的 36 倍。

经过长时间的科研攻关，清华紫光在信息安全领域终于取得了技术性突破，其产品紫光 S 锁已经进入实际应用阶段。S 锁可以对存储在计算机内的重要文档进行深层加密保护，全面防范来自各方面的对信息安全的威胁。

和其它安全产品相比紫光 S 锁还具备以下出色的优势：

1．新颖的硬件钥匙形式

2.高强度、多层次的安全性

3.动态实时的加密/解密

4.独特的计算机开发系统锁定技术

5.简单易用

		普通产品	紫光 S 锁
安全层次		应用层上开发，容易被破坏和解密	操作系统底层开发，保证了足够的安全性以及加密解密的高效率
安全强度	正常状态	无硬件，身份验证和算法均为软件易攻破	有硬件保护，身份验证和算法都通过硬件钥匙，攻击难度大
	突然断电或死机时	被解密的保密文件可能暴露在硬盘中	任何情况下，硬盘中的保密文件总是密文

为了加强信息安全保障工作，就必须大力加强信息安全技术的研究、开发，促进国内信息安全产业的发展，国务院信息化工作办公室（简称“ 国信办 ”）发布的第 27 号文件，明确了加强信息安全工作的指导思想和原则，确定了今后一段时间的重点任务，是我国信息安全建设和管理的重要指导性文件。

27 号文件以“ 三个代表 ”重要思想为指导，坚持“ 积极防御、综合防范 ”的方针，通过 27 号文件，实现提高信息安全防护能力，重点保障基础信息网络和重要信息的安全，创建安全、健康的网络环境，保障和促进信息化发展，保护公众利益，维护国家安全。国家财政资金建设的信息化项目，要优先采用国产软件、设备和服务。规范信息安全市场环境，支持我国信息安全产业的发展，形成我们自己的信息安全产业，摆脱信息安全关键技术与市场受制于人的被动局面，提高信息安全防护水平。

清华紫光股份有限公司
TSINGHUA UNISPLENDOUR CO.,LTD.
中国 北京 清华大学紫光大厦 邮编(zip):100084
电话：(010)62701188 传真：（010）62773007
网址:http://www.thunis.com