

# 亚略特信息安全等级保护

## 指纹识别解决方案

- 中国生物识别标准制定单位
- 中国最值得信赖生物识别品牌
- 指纹信息安全市场占有率NO.1

# 目 录

前言：巩固信息安全 保密责任重于泰山.....	5
1、信息安全危机四伏.....	5
2、身份认证 – 信息安全关键环节.....	6
3、指纹身份认证 — 信息安全等级保护要求强化机制.....	7
4、生物识别技术在信息安全中的意义.....	8
亚略特 — 指纹信息安全防护专家.....	9
亚略特信息安全产品体系.....	10
第一篇 涉密移动存储介质管理解决方案.....	11
产品一 亚略特天工系列指纹保密U盘.....	14
1、FKS680 标准版指纹保密U盘.....	14
2、FKS680 防木马版指纹保密U盘.....	16
产品二 亚略特安全保密U盘.....	17
1、BMU900 防木马版安全U盘.....	17
2、BMU900 标准版安全U盘.....	18
产品三 亚略特天盾系列指纹安全硬盘.....	19
1、亚略特天盾指纹安全硬盘 产品介绍.....	19
2、产品特点.....	19
3、适用范围.....	20
4、功能描述.....	20
第二篇 内网安全管理指纹识别解决方案.....	21
产品四 亚略特终端与内网安全管理系统.....	22
1、系统架构图说明.....	22
2、系统功能特点.....	23
3、终端与内网安全管理系统登陆界面.....	23
产品五 指纹单机防护：亚略特指纹电脑安全卫士.....	24
1、应用背景.....	24
2、指纹电脑安全卫士选型介绍.....	24
产品六 亚略特基于指纹识别的终端安全登陆系统.....	25

1、应用背景.....	25
2、系统价值.....	25
3、系统功能特点.....	26
4、指纹AD域系统网络结构图 .....	26
<b>第三篇 安全接入管理指纹识别解决方案 .....</b>	<b>27</b>
产品七 亚略特虚拟化身份安全指纹认证系统 .....	28
1、虚拟化应用面临的诸多安全挑战 .....	28
2、指纹虚拟化身份安全系统介绍 .....	28
3、指纹虚拟化身份安全系统网络部署架构图 .....	28
4、指纹虚拟化身份安全系统特点 .....	29
5、指纹登陆虚拟化的两种方式 .....	29
产品八 亚略特指纹SSL VPN远程访问系统 .....	30
1、指纹SSL VPN系统介绍 .....	30
2、指纹SSL VPN系统价值 .....	30
3、指纹SSL VPN系统网络架构图 .....	30
产品九 亚略特指纹单点登陆管理系统 .....	31
1、指纹单点登陆系统介绍 .....	31
2、指纹单点登陆系统价值 .....	31
3、指纹单点登陆系统功能特点 .....	31
<b>第四篇 身份鉴别管理指纹识别解决方案 .....</b>	<b>32</b>
产品十 TrustLink 指纹身份认证平台 .....	33
1、TrustLink平台介绍 .....	33
2、TrustLink指纹身份认证平台功能 .....	34
3、TrustLink 指纹身份认证平台特点 .....	35
(1) 五种安全防范机制 .....	35
(2) 灵活的平台扩展能力 .....	35
(3) 完善的安全策略 .....	35
(4) 安全便捷的后台管理 .....	36
(5) 超强的组件化设计能力 .....	36
4、TrustLink Web Service 网络指纹认证管理 .....	37

产品十一 亚略特指纹数字签名身份安全管理 .....	38
1、传统PKI应用背景 .....	38
2、亚略特指纹USBKEY产品介绍 .....	39
3、功能特点.....	39
TrustLink 指纹采集终端选型指南 .....	40
第五篇 亚略特资质荣誉及典型案例.....	41
一、亚略特 资质荣誉证书.....	41
二、亚略特 信息安全典型案例.....	45

## 前言：巩固信息安全 保密责任重于泰山

### 1、信息安全危机四伏

#### (a) 数据调研

中国	全球
95% 95%网络中心受过黑客侵袭	79秒 身份盗窃每79秒发生一起
58% 公安部调查58%企业网络有隐患	50% 未采取加密机制的组织平均多付出50%财务和运营资源
28.5% 28.5%网民评价互联网安全性差	80% 80%安全漏洞来自与密码相关的身份认证

以上数据源自Gartner、iResearch等权威机构

#### (b) 危机事件回放






##### 事件一

某研究所几十位工程技术人员存在硬盘上辛苦三年研发的成果一夜被盗走，其中包括多项国家秘密项目设计图纸、系统组成、性能和工作方式等，给国家安全带来不可估量的损失。

##### 事件二

美国海军监审部门内部报告显示，美国太平洋舰队的战舰及潜艇上共丢失近 600 部电脑，其中 14 部用于处理保密数据。丢失的电脑中存有大量敏感信息，不仅威胁美国国家安全，也对美国海军声誉造成玷污。

#### (c) 信息安全现状

				
涉密牵动国家安全	电子化日益深入	系统中大量业务机密	口令密码隐患重重	管理手段亟待升级

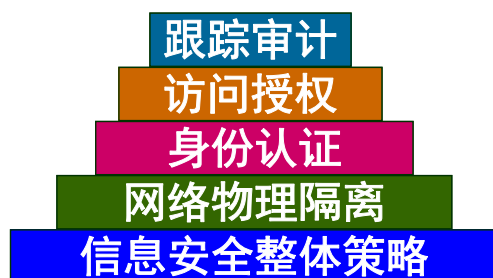
- 受国际信息间谍、敌对势力、恐怖集团、信息战攻击影响，保障涉密单位信息安全和防破坏性尤其具有战略意义。
- 各级党政机关、国防军工单位、企事业单位普遍建立办公自动化、电子政务、文档管理等信息系统，实现计算机单机或网络办公，业务中涉及大量国家秘密数据。
- 用户名+密码的系统登录或网络身份鉴别方式，甚至不设密码、长期不更换密码或直接将密码保留在对话框内等现象，为涉密系统和机密数据造成安全隐患。
- 了解安全管理是否有效贯彻，安全运作流程是否有效实施，打破主观意志和经验处理的瓶颈，实现安全管理可视化和具体衡量，涉密单位亟需借助更先进的技术手段。

## 2、身份认证 — 信息安全关键环节

“组织内部正在大力建设信息安全体系时，很容易忽略最重要也最容易被忽略的 — 身份认证环节。”

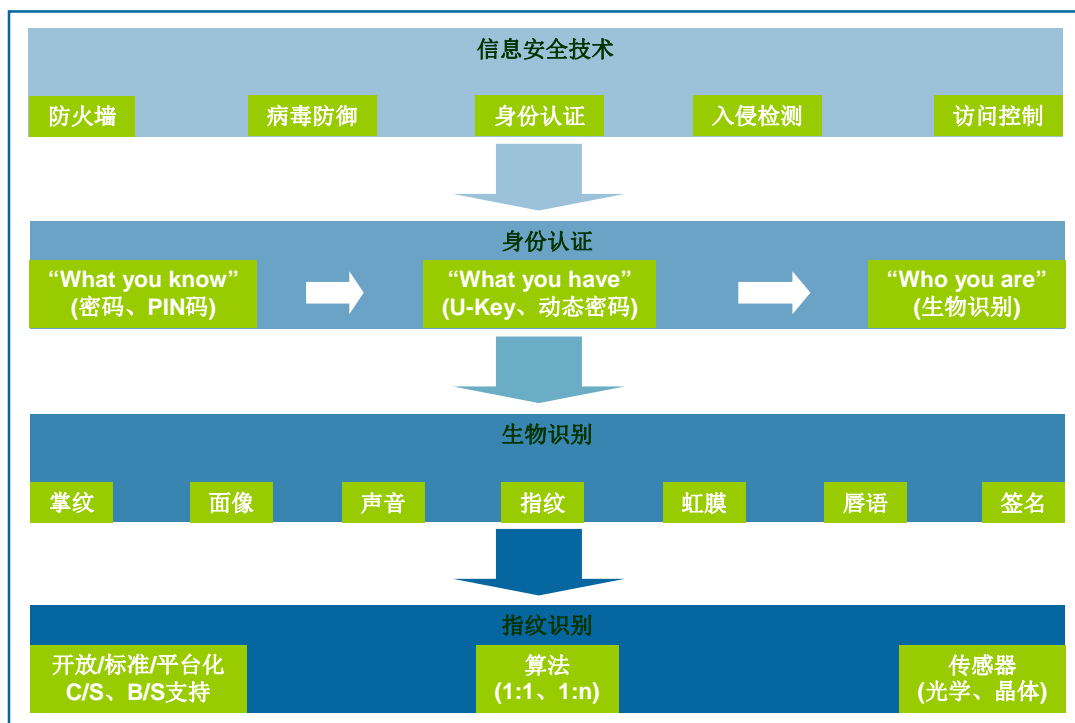
— 引自国家保密局某局长在保密工作会议上的讲话

### (a) 身份认证 — 信息安全的各个环节



在信息安全体系中，身份认证是一个非常关键的环节，也是整体信息安全的前提，而原有的“用户名+密码”的身份识别方式仍被沿用至今。有数据表明，信息安全面临的主要威胁不是来自于外部攻击，85%的安全漏洞其实来自于企业和组织内部。包括了信息系统制度流程的建设、人员安全意识的提高、安全技术的应用等各方面的因素。其中，传统的密码身份认证所存在的安全缺陷和非人性化且记忆不方便是一种重要的原因。

### (b) 身份认证决策树



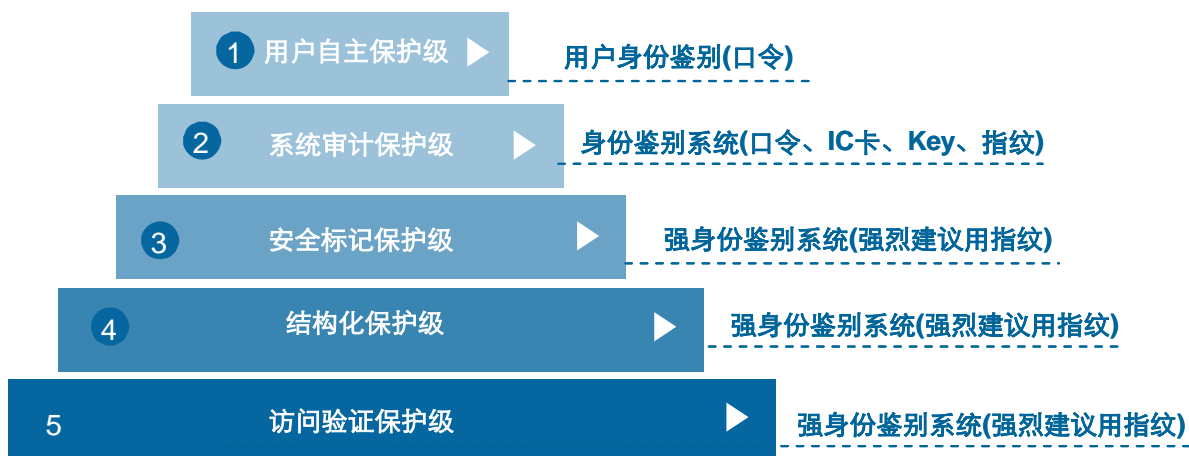
由图可看出，生物识别已经成为安全与便捷身份认证的最佳选择，而指纹识别因其易用性强、普及性广、技术不断成熟，已成为当前生物识别领域的主流身份认证技术。



### 3、指纹身份认证 —— 信息安全等级保护要求强化机制

随着信息技术的大规模应用，信息安全的重要性与日俱增，政府、安全、保密、军工军队等涉密领域面临日趋严重的移动存储泄密风险和信息安全漏洞。

由此，国家相关政策与法规陆续出台，《中华人民共和国计算机信息系统安全保护条例》、《涉及国家秘密的信息系统分级保护技术要求》、《信息系统安全等级保护基本要求》、《信息系统安全等级保护测评准则》，《计算机信息系统安全等级保护（通用技术要求）》，明确规定我国“计算机信息系统实行安全等级保护”，各级计算机信息系统须有用户身份鉴别功能设计，并在三级以上系统“要求有更加严格的身份鉴别，如采用人体生物特征（指纹、视网膜）等特殊信息进行身份鉴别，并在每次用户登录系统之前进行鉴别”。



#### 信息安全等级划分及身份鉴别要求









《信息系统安全等级保护定级指南》中可获知，信息安全保护从第一级安全保护环境开始，便提出安全功能必须具备用户身份鉴别功能设计。自二级开始，为增强系统的安全保护能力，安全保护环境中身份鉴别要求升级为身份鉴别系统。自三级开始，要求除了采用口令外，强烈建议使用指纹识别等人体特殊信息进行强身份鉴别。

亚略特是中国最专业的指纹信息安全方案提供商，依靠自主知识产权的指纹动态优化算法和生物识别加密技术两大核心技术，按照等级保护和分级保护的要求，从军队、保密、军工企业等众多涉密企业的实际需求出发，研发出了一套完整的基于指纹识别信息安全等级防护方案，方案涵盖了指纹安全存储介质、指纹计算机安全防护、指纹 AD 域身份鉴别、应用系统指纹识别、指纹 USBKEY 等需要指纹鉴别的各种应用领域，大大增强用户身份鉴别的强度、数据保密性和身份可信审计等，最大程度降低泄密风险。

#### 4、生物识别技术在信息安全中的意义

生物识别（biometrics）是利用人体生物特征（如指纹、虹膜、声音等）进行身份认证的一种技术，与传统的“帐号+密码”（what you know）或持卡（what you have）认证模式相比，生物识别直接验证用户本人，即 who you are。

生物识别以指纹为例，指纹识别特点：

唯一	目前世界上未发现两枚相同的指纹。相同指纹出现的机率为50亿分之一以上。		
随身	生理特征随身携带，随时随地使用。		
稳定	指纹在母胎中三至四个月时已形成，至14岁左右完全定型，之后不随时间而改变。		
方便	与随身性相呼应，指纹无需记忆或额外携带，不会遗失。		
成熟	指纹以其精确、易取等优势成为生物识别技术中的主流。		
安全	不击键	不通过键盘输入	 键盘跟踪/木马
	看不懂	输入的实际密码已被“刷指纹”替代	 密码偷窥
	借不了	无法让渡或转让	 （被动）人情泄密
	说不清	无法口述告知	 （主动）口误泄密
	不需记	将传统密码设置得长而复杂	 恶意穷举破解
	盗不走	设备失窃时数据仍然安全	 失窃泄密
	丢不了	丢失设备时数据仍然安全	 丢失泄密
	很难破 ★	业界领先技术（如硬加密+指纹认证等）	 超级黑客

几种身份认证模式比较，指纹识别的优势：

类别	应用特点	安全	方便	执行力★
帐号密码	需要记忆/易丢失/易被盗、破解、侦听/可以转让	★★	★★★	★
IC卡	需要携带/易丢失/易被盗、破解、侦听/可以转让	★★★	★	★★★
动态口令	需要携带/易丢失/使用繁琐/可能被盗/可以转让	★★★	★	★★★
USB KEY	需要携带/易丢失/使用繁琐/可能被盗/可以转让	★★★	★	★★★
生物识别	不需记忆/不丢失/不易被盗、破解、侦听/无法转让	★★★★	★★★★	★★★★

以“物”为介质的认证时代，物品本身成为授信凭证，一经转让、丢失即可导致相应的权限转让或外泄。生物识别“人证合一”要推行，要求授权于受权人时真实统一，管理执行严密无缝。



## 亚略特 — 指纹信息安全防护专家

亚略特是中国领先的专业指纹识别技术和身份安全解决方案提供商，致力于通过自主创新的指纹生物特征识别技术，解决政府、军工等涉密领域广泛存在的身份泄露、数据泄密等信息安全问题。

亚略特拥有数十项领先的自主知识产权专利技术，并自主研发了指纹信息安全硬件产品（天工系列指纹保密U盘、天盾系列指纹安全硬盘、天行系列指纹鼠标和指纹仪等）及TrustLink指纹身份认证平台软件。亚略特全线信息安全产品均已通过公安部“信息安全专用产品”、中国人民解放军“军用信息安全产品”、国家保密局“涉密信息系统产品”等权威安全资质认证和国际高标准FCC、CE认证。凭借卓越的技术成就和良好的市场口碑，亚略特荣获“中国信息安全最值得信赖生物识别品牌”的美誉。

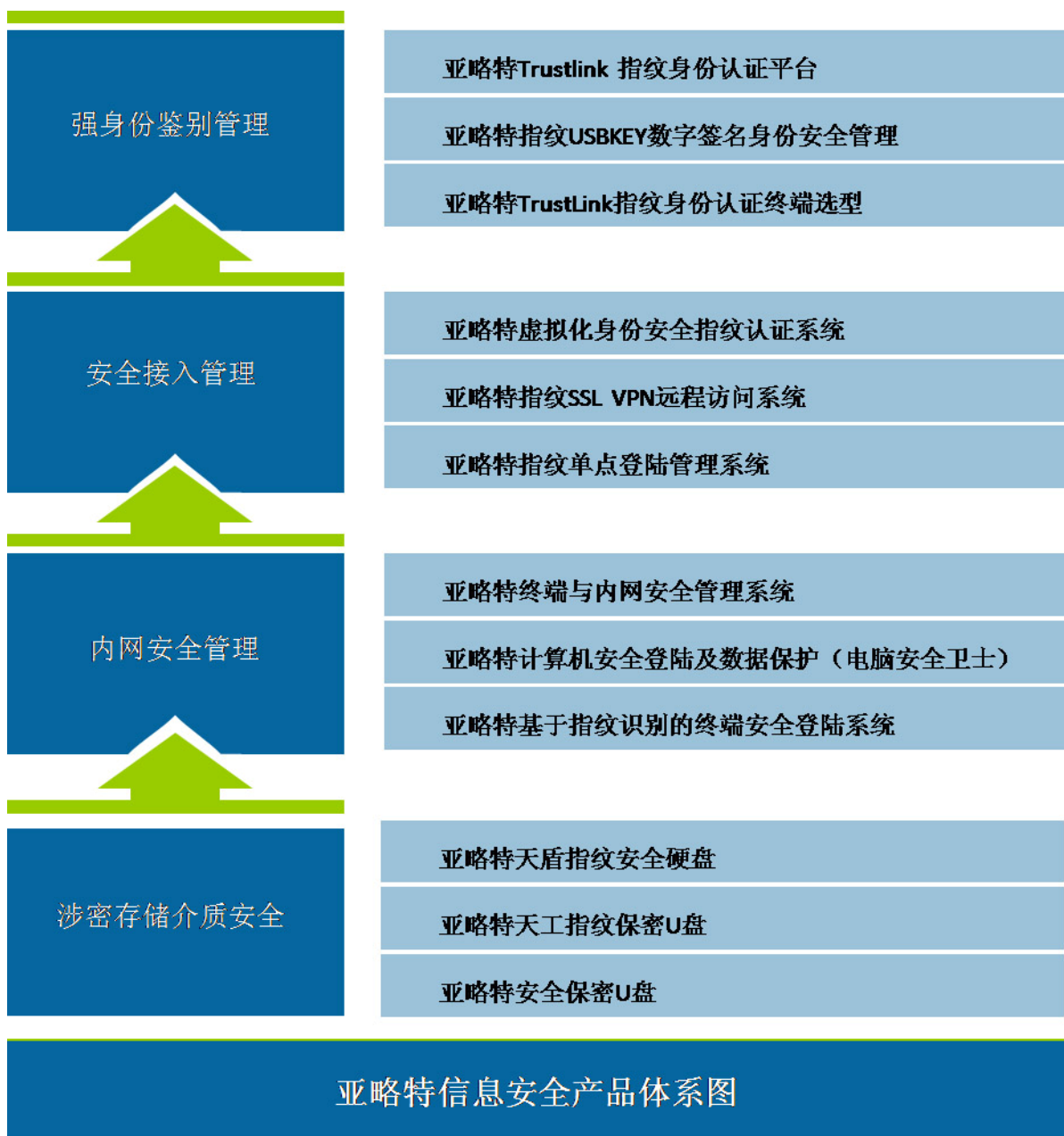
在中国，亚略特是服务于电子政务、电子军务、涉密信息安全领域最专业、最值得信赖的生物识别企业，众多国家部委、政府保密安全部门以及国防军工单位选择了亚略特专业的指纹产品和身份安全应用解决方案。



## 亚略特信息安全产品体系

根据《涉及国家秘密的信息系统分级保护技术要求》和《信息系统安全等级保护基本要求》，条例规定应采用生理特征如指纹、虹膜等强身份鉴别方式进行身份鉴别，有效杜绝和禁止涉密数据外泄。

亚略特认为，身份鉴别是一个安全管理问题，涉及存储介质管理、计算机安全登录管理、文件管理、网络化平台管理等，必须从状态、行为、事件三方面来进行防御。因此，《亚略特信息安全等级保护指纹识别解决方案》，以业务流运作过程中“权责分配落实到技术”为依据和保障，重点从涉密存储介质安全管理、涉密内网安全管理、涉密信息系统安全接入、信息安全等级应用系统网络指纹身份认证，四大方向来阐述了指纹身份识别信息安全的 application 情况。



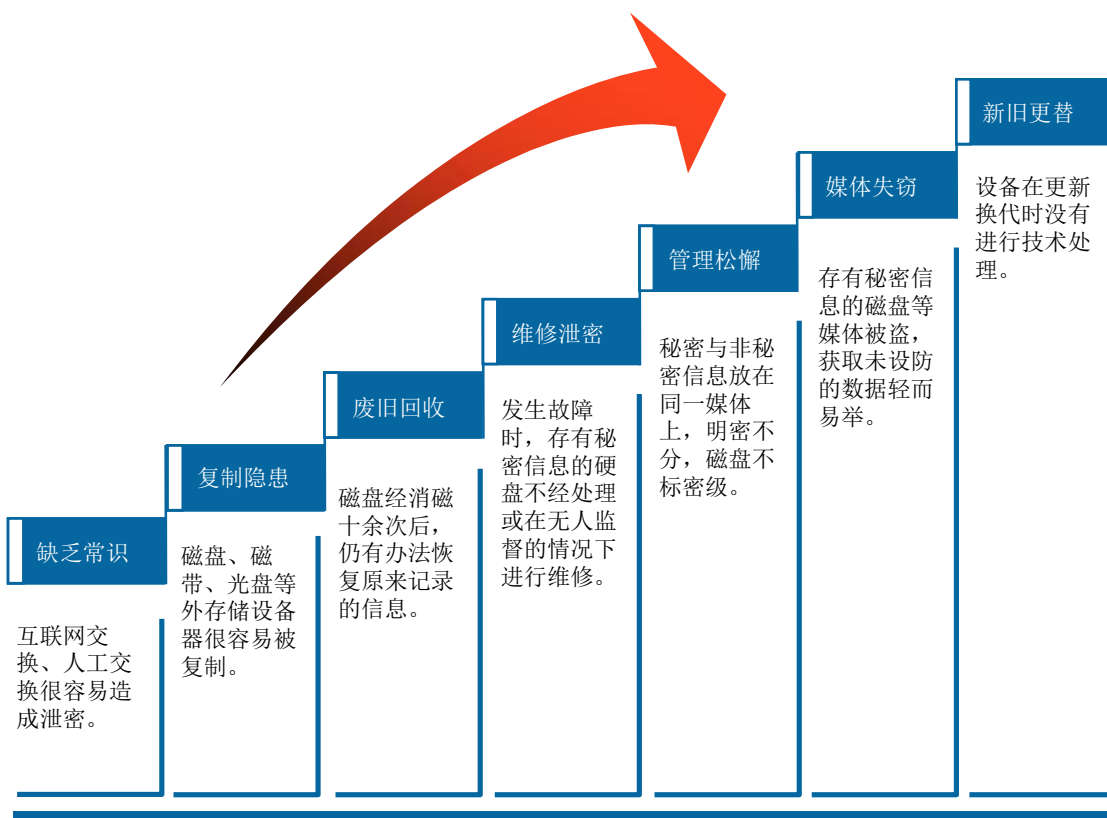
## 第一篇 涉密移动存储介质管理解决方案

### 1、由数据交换引发的信息安全问题

移动存储介质由于体积小、容量大等优点，在信息安全行业广泛使用。但是，普通移动存储介质作为涉密数据和信息交换的重要载体，在信息安全存储方面存在极大的安全隐患：

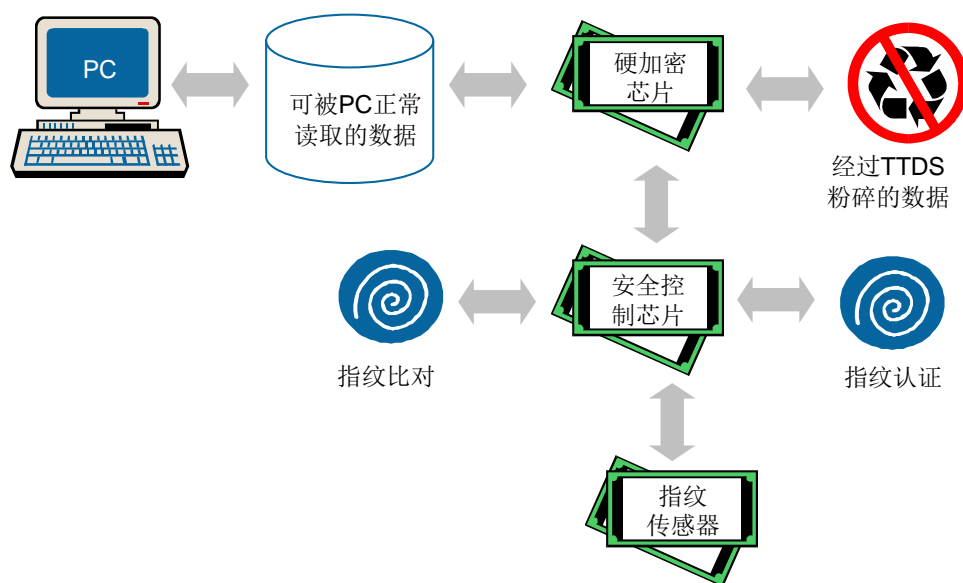
1 管理无序 ▶	涉密移动存储介质未建立严格的登记、使用、销毁制度，处于不管不问状态；
2 明密不分 ▶	涉密移动存储介质中数据未采取分类管理，涉密与非密，甚至个人信息共存；
3 公私不分 ▶	单位配发的和个人自购的移动存储介质混用，公私不分；
4 用途不明 ▶	具有娱乐功能的介质被用于存储涉密信息，既娱乐又办公；
5 混插混用 ▶	涉密移动存储介质在内网、外网和公众网混插使用现象普遍。

越来越多的秘密数据和档案资料存储在计算机里，附载在磁性介质和光学介质上，存储在没有任何防护机制的介质里，涉密数据将面临“风险不可控、过程不可视、事故无从追”的风险境地。



## 2、亚略特涉密移动存储介质 体系结构

亚略特指纹涉密移动存储介质，使数据存储装上了一道安全之门，保护重要信息，减缓意外泄密风险，减少丢失、盗窃等原始手段的数据流失。从容捍卫机密信息，打击无所不在的窃密侵犯，谢绝一切暴力窃密、技术破解。



## 3、技术说明

活体识别	测量人体真皮组织电特性，不受手指干、湿、脏或磨损影响，杜绝橡胶手指。
指纹绑定密钥	通过指纹与密钥绑定的方式，隐藏存储加密密钥。
数据强保护机制	硬件级芯片采用数据强保护机制，可对数据进行实时加解密。
内嵌保密标识	芯片内置唯一设备 PID 编号，密级标识与信息主体绑定，方便安全监管。
反跟踪反编译处理	提升系统健壮性，有效防范降低破解风险。
自主指纹算法	亚略特 Bione 动态优化算法，BE 生特识别加密技术，识别精准、加密牢固。
断电自动保护	实时侦测存储介质当前工作状态，一旦断电或者 USB 断连则自动加锁。
安全交接	使硬盘的管理权在不同用户间实现安全交接，确保重要数据的权限控制。
系统兼容性	亚略特全线指纹涉密移动存储介质支持与第三方标签系统接入。例如：鼎普、北信源、南京才华、金城保密、广州国脉、山东朗威、山东中孚、北京博睿勤、北京华旗资讯、上海格尔、北京万里红等。

#### 4、亚略特指纹存储设备 产品优势



- 以自主创新为核心竞争力，拥有多项国家专利，部分尖端技术领先世界，缔造国际市场上强势民族品牌。
- 全线产品通过公安部、国密、军密等权威机构认证，列入部分省市涉密采购推荐品牌。
- 产品研发遵循 CMM 规范，有效提升效率，保障质量。
- 产品设计符合涉密信息安全管理要求，功能实用可靠。
- 政府、军工军队、安全保密等涉密领域客户超过 1000 家。

#### 亚略特指纹涉密存储设备与普通指纹存储设备 比较

		亚略特指纹涉密存储设备	普通指纹存储设备
硬件工艺	指纹芯片	全线采用活体指纹识别晶体电容传感芯片	☑
	芯片支持	可灵活选择不同厂家指纹传感、控制器芯片	☑
	物理安全	高可靠物理防尘、防震、防水	☑
基本功能	即插即用	无需安装硬件驱动程序	☑
	自动运行	程序内嵌在硬件内，连接电脑时自动运行	☑
	指纹管理	创建、更改和删除用户指纹，最长达10枚	☑
	指纹锁盘	只有指纹认证通过后才能打开安全存储空间	☑
	文件加密	用“指纹+密钥”方式加密文件	☑
安全机制	指纹保护密钥	指纹信息与随机码相结合，密钥唯一且随机	☑
	指纹算法	支持AES、3DES多种加密算法，支持第三方算法嵌入	☑
	硬件加密	采用芯片级加密技术	☑
	递归加密	支持文件、文件夹双层加密，或多指递归加密	☑
	文件粉碎	彻底删除涉密文件，不留任何痕迹	☑
	安全交接	新老用户移交设备时需同时进行指纹认证	☑
	日志审计	对使用过程进行记录和追踪,可进行稽核审计	☑
	断电保护	遇断电或USB断连，即自动置于加锁状态	☑
	* 多指认证	设定同时需有多枚指纹匹配成功方可使用U盘	☑
	* 断网保护	使用设备时对网络进行自动断联保护	☑
分级管理	* 密级标识	设有秘密/机密/绝密标识，便于介质管理	☑
	* PID管理	内置唯一PID编号，PID与设备绑定，不可篡改。	☑
扩展应用	* 第三方应用	可提供开发接口，快速集成第三方应用。	☑
	* 网络应用	结合TrustLink支持网络指纹认证，升级应用安全	☑

- 1、以上所列功能特性非亚略特指纹存储设备统一标配；
- 2、\*所标注的信息为指纹存储设备的可选功能。



## 产品一 亚略特天工系列指纹保密U盘

亚略特天工指纹保密 U 盘，面向信息安全保密高端市场量身定制，以卓越硬件品质、工业级设计、安全技术、满足用户高效、存储安全性管理的需要，是一款高性能、高安全的指纹安全产品。天工指纹保密 U 盘为纯银金属外观，滑盖式结构有效保护指纹传感器免受物理伤害，创新横向手指滑动设计，更加符合人体工学，采集指纹更舒适方便。

结合国内涉密领域应用特点，天工指纹保密 U 盘采用了活体指纹识别、设备 PID 标识管理、亚略特 BE 生物识别加密技术、高强度加密机制等多重安全技术，提供指纹保护 U 盘、指纹保护文件、文件粉碎、指纹安全交接、多人指纹管理等功能，全面防卫指纹移动存储的身份安全、数据安全、管理安全。

亚略特天工指纹保密 U 盘分为：FKS680 标准版和 FKS700 防木马版，适用于党政机关、军工\军队、大型企事业单位等涉密信息移动存储及管理需求



型号：FKS680

### 1、FKS680 标准版指纹保密U盘

#### 1.1 产品特点

##### ☞ 采用活体指纹识别安全模块

A 级闪存芯片，通过手指真皮层获取手指持续有效的特征值数据，提高使用安全性。

##### ☞ 独创指纹安全密钥绑定技术

独有的指纹保护密钥机制，通过指纹与密钥绑定的方式，隐藏存储加密密钥。

##### ☞ 内嵌唯一保密标识实现安全监管

芯片内置唯一设备 PID 编号，密级标识与信息主体不可分离，方便安全监管。

##### ☞ 对数据流进行强保护机制

采用硬件加密技术，对数据进行实时强保护，有效控制数据的可见范围。

##### ☞ 有效的反跟踪、反编译处理

反跟踪和反编译技术的采用，有效防范和降低系统的破解风险，提升健壮性。

##### ☞ 使用便捷，节省用户时间

无须安装驱动，即插即用型，指纹程序自动运行。



## 1.2 功能描述

指纹管理	通过创建、修改、删除等指纹库管理，可实现多人同时使用。
系统设定	对保密 U 盘相关参数进行系统设置。
指纹锁盘	只有指纹认证通过后才能打开安全存储空间，杜绝他人非法使用。
文件保护	用“指纹+密钥”方式加密所需保护的文件。
搜索文件保护	搜索当前电脑上用户加密过的文件，方便、快捷。
文件粉碎	彻底删除涉密文件，不留任何痕迹。
安全交接	新老用户移交设备时需同时进行指纹认证，实现设备安全交接。
信息备份	通过指纹认证后备份系统密钥、指纹等信息，防止设备遗失后无法打开加密文件。
日志审计	对保密 U 盘使用的过程进行记录和追踪，可进行稽核审计。
断联保护	运行指纹设备管理系统时，自动断开网络连接；退出指纹设备管理系统后，自动恢复网络联接。
互联网检测	自动检测互联网联结状态，限制指纹设备的安全区在互联网连接状态下使用。
电子文件保险柜	在电脑中建立电子文件保险柜，只有通过指纹认证，才能打开电子文件保险柜存储文件，关闭后自动隐藏，安全、便捷。

## 2、FKS680 防木马版指纹保密U盘

### 2.1 产品特点

- 自解密密码认证，高强度密码保护机制
- 指纹保密 U 盘分为交换区和内网区分区存储，内外网分开使用
- 隐藏用户存储空间，在 Windows 系统中不会出现用户存储空间的盘符
- 采用自主研发的文件系统，限制操作系统对设备的访问范围，防止病毒木马感染
- 产品无须安装驱动，即插即用型，加密程序自动运行
- 审计信息记录在指纹 U 盘本地的审计区，以供分析

### 2.2 功能描述

指纹登陆磁盘	通过指纹身份认证打开磁盘安全存储区。
指纹管理	通过创建、修改、删除等指纹库管理，可实现多人同时使用。
分区存储	设备可分为交换区和内网区分开存储。
文件操作	可复制、剪切、粘贴、删除、重命名、新建文件夹。
设备格式化	提供用户快速删除分区文件、恢复分区初始状态的操作。
日志审计	记录包括用户名、操作类型、源文件名、目标文件名、操作时间等；环境记录包括 Windows 用户名、Windows 版本号、计算机名、计算机 IP 地址、网卡物理地址、机器码、硬盘序列号、日志来源等。
系统设定	对磁盘运行相关参数进行配置。

## 产品二 亚略特安全保密U盘

亚略特 BMU900 安全保密 U 盘，面向政府、军队、军工、企事业单位等高保密市场量身定制，以其卓越的性能指标满足涉密领域移动存储介质的高可靠性、高加密性要求。

BMU900 安全保密 U 盘利用高强度加密算法对 U 盘进行强保护机制设置，用户需要通过输入口令密码才能进入 U 盘，读取 U 盘内的数据资料。

与此同时，为杜绝病毒木马直接操作设备存储区域的可能，BMU900 安全保密 U 盘将限制操作系统对设备的访问范围，系统无法识别移动存储设备的盘符，病毒木马也就无法自动运行。



型号：BMU900

### 1、BMU900 防木马版安全U盘

#### 1.1 产品特点

- 自解密密码认证，高强度密码保护机制
- 安全保密 U 盘分为交换区和内网区分区存储，内外网分开使用
- 隐藏用户存储空间，在 Windows 系统中不会出现用户存储空间的盘符
- 内置加密芯片对数据流进行透明加密
- 采用自主研发的文件系统，限制操作系统对设备的访问范围，防止病毒木马感染
- 产品无须安装驱动，即插即用型，加密程序自动运行
- 审计信息记录在 U 盘本地的审计区，以供分析

#### 1.2 功能描述

登陆磁盘	通过口令密码认证打开磁盘安全存储区。
分区存储	设备可分为交换区和内网区分开存储。
文件操作	可复制、剪切、粘贴、删除、重命名、新建文件夹。
设备格式化	提供用户快速删除分区文件、恢复分区初始状态的操作。
日志审计	自动记录用户使用操作记录，通过日志管理进行稽核审计。
系统设定	对磁盘运行相关参数进行配置。

## 2、BMU900 标准版安全U盘

### 2.1 产品特点

- ☉ 芯片内置唯一设备 PID 编号，密级标识与信息主体不可分离，方便安全监管
- ☉ 安全保密 U 盘分为公开区和安全区分区存储
- ☉ 采用高效的反跟踪、反编译处理技术，防范和降低系统的破解风险
- ☉ 产品无须安装驱动，即插即用型，加密程序自动运行
- ☉ 审计信息记录在 U 盘本地的审计区，以供分析

### 2.2 功能描述

登陆磁盘	通过口令密码认证打开磁盘安全存储区。
文件保护	通过密码对文件进行加密设定，保护机密资料和个人文件安全。
搜索文件保护	搜索当前电脑上用户加密过的文件，方便、快捷。
文件粉碎	彻底删除涉密文件，不留任何痕迹。
安全交接	新老用户移交设备时需同时进行口令认证，实现设备安全交接。
身份有效时间	通过一次密码身份验证后，在用户设定的密码使用有效时间内，执行各功能无需再进行身份确认。
日志审计	自动记录用户使用操作记录，通过日志管理进行稽核审计
断联保护	运行设备管理系统时，自动断开网络连接； 退出设备管理系统后，自动恢复网络联接。
互联网检测	自动检测互联网联结状态， 限制设备的安全区在互联网连接状态下使用。
电子文件保险柜	在电脑中建立电子文件保险柜，只有通过口令认证， 才能打开电子文件保险柜存储文件，关闭后自动隐藏，安全、便捷。

## 产品三 亚略特天盾系列指纹安全硬盘

### 1、亚略特天盾指纹安全硬盘 产品介绍

由亚略特自主研发全球领先的天盾指纹安全硬盘，是专门针对目前军队、政府等保密系统普遍存在的移动存储安全漏洞、隐患而设计的指纹安全移动存储产品，最大容量可以达到 500G。该产品集多项创新技术于一体，更以十项指标全球领先，成为指纹应用高端市场精品代表。



型号：FDS250

作为全球领先的指纹硬盘方案，天盾指纹安全硬盘提供牢固可靠的安全应用，从物理层三重屏蔽强化抗静电、抗电磁辐射，到逻辑层 BE 指纹加密、片内数字签名、片内数据加密等多项技术，全面防卫指纹移动存储的身份安全、数据安全、管理安全。

产品整体厚度 14.4mm，堪称目前最薄的指纹硬盘，全线采用金属氧化喷砂表面处理工艺，形成独特纯黑色质感外观；独立第三方测评“六道工序五重检验，半成品后每道工序全检”机制，确保硬件品质卓越，出类拔萃。

### 2、产品特点

- ☞ 整合电感式指纹传感器，同时采用稳定度、省电性、速度综合指标最佳的控制器
- ☞ 所采用芯片全部为无铅芯片，符合欧盟 ROHS 指令
- ☞ 反应更敏捷，每 62ms 进行一次手指检测
- ☞ 指纹采样速率更高，每秒可读 160 幅指纹图像
- ☞ 功耗更节约，动态功耗节约 50%，静态功耗节约 99%
- ☞ 读写速度更迅捷，写入 14 兆 B 每秒，读取 22 兆 B 每秒
- ☞ 氧化喷砂纯黑表面，极具质感却不易沾染油渍或污痕
- ☞ 基于人体工学的 15° 倾斜凹槽，令手指滑动舒适
- ☞ 内置弹性钢片强化抗震功能，1ms 以内承受 900G 的外力
- ☞ 先进噪音控制技术，平均音量 15 分贝荣膺静音之王

### 3、适用范围

- ☉ 党政机关、军工军队涉密信息移动存储及管理需求
- ☉ 大容量机密文件，指纹加密应用
- ☉ 税务工商、公安、警务、电力、交通等行业安全存储需求

### 4、功能描述

指纹管理	通过创建、修改、删除指纹库，可实现多人同时使用。
系统设定	对指纹安全硬盘相关参数进行系统设置。
指纹锁盘	只有指纹认证通过后才能打开安全存储空间，杜绝他人非法使用。
文件保护	用“指纹+密钥”方式加密所需保护的文件。
搜索文件保护	搜索当前电脑上用户加密过的文件，方便、快捷。
文件粉碎	彻底删除涉密文件，不留任何痕迹。
安全交接	新老用户移交设备时需同时进行指纹认证，实现设备安全交接。
信息备份	通过指纹认证后备份系统密钥、指纹等信息，防止设备遗失后无法打开加密文件。
日志审计	对使用过程进行记录和追踪，可进行稽核审计。
断联保护	运行指纹设备管理系统时，自动断开网络联接；退出指纹设备管理系统后，自动恢复网络联接。
互联网检测	自动检测互联网联结状态，限制指纹设备的安全区在互联网连接状态下使用。
电子文件保险柜	在 PC 中建立电子文件保险柜，只有通过指纹认证，才能打开电子文件保险柜存储文件，关闭后自动隐藏，安全、便捷。



## 第二篇 内网安全管理指纹识别解决方案

### 1、背景分析

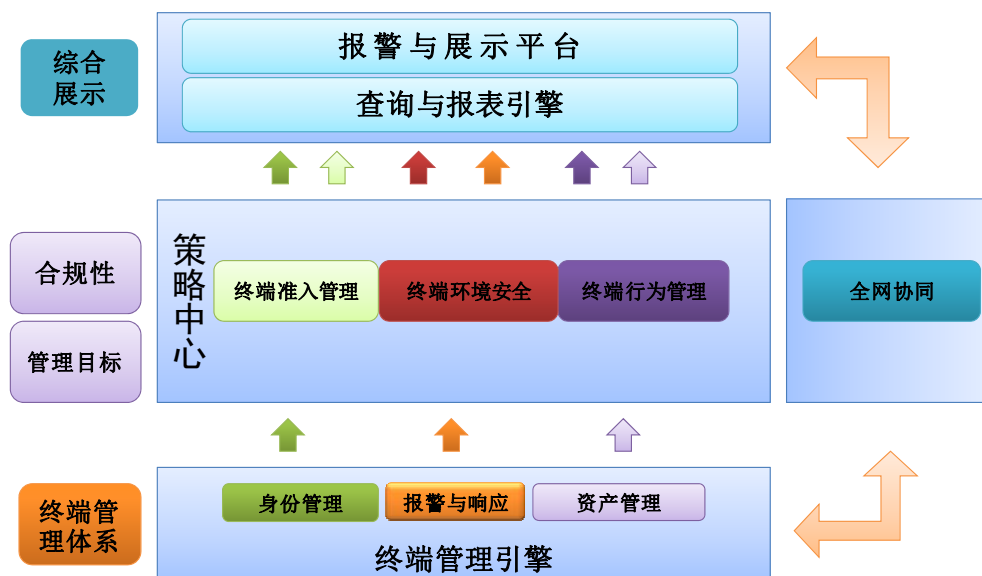
计算机系统安全包含实体安全、运行安全和信息安全。其中信息安全又涉及操作系统安全、数据库安全、网络安全、访问控制、信息加密和身份鉴别。由于被国际著名的几家技术提供商所把持，操作系统与数据库的安全显得被动而没有选择；网络安全普遍视病毒与黑客为焦点，在保障信息安全的作用上，仍然偏向于“环境安全”。

我们看到，网络安全已成为阻碍网络应用的关键所在，要使企事业单位的 IT 资源能够得到有效的利用，首先需要解决的是基本的网络安全威胁。值得欣喜的是，网络安全得到越来越多人的重视，已经有许多企业在网络边界部署了防火墙，网络中安装了杀病毒软件，部署了入侵检测、身份认证、漏洞扫描等系统来防止外界威胁。然而，这些安全措施并没有对内网，尤其是没有对各个计算机终端进行有效监控，从而无法避免内部 IT 资源滥用、内部网络信息泄露、内部员工的故意攻击等问题，更不能对各种因内部因素产生的网络安全问题进行有效的预防、监控和审计。我们总结了一下，来自内网的安全威胁主要有以下几个方面：

- 第一，内部人员或设备的主动或者被动泄密
- 第二，内部人员主动或被动的制造/传播病毒等恶意代码
- 第三，非授权使用或者授权滥用
- 第四，内部人员或者设备的主动或者被动攻击
- 第五，因安全管理不善，引发的 IT 资源不可用或者资源损失
- 第六，客户机自身存在安全缺陷，导致网络内部安全隐患

信息安全专家亚略特认为，最根本的信息安全其实表现在信息的存储与日常使用，即信息安全的后三类“访问控制”、“信息加密”和“身份鉴别”，我们将其归纳为“信息加密”和“身份认证”。信息加密使得数据在最危险（如丢失或被未授权获取）情况下能够获得相对安全，身份认证则是信息安全领域一直以来的短板。

### 2、亚略特内网安全管理系统结构

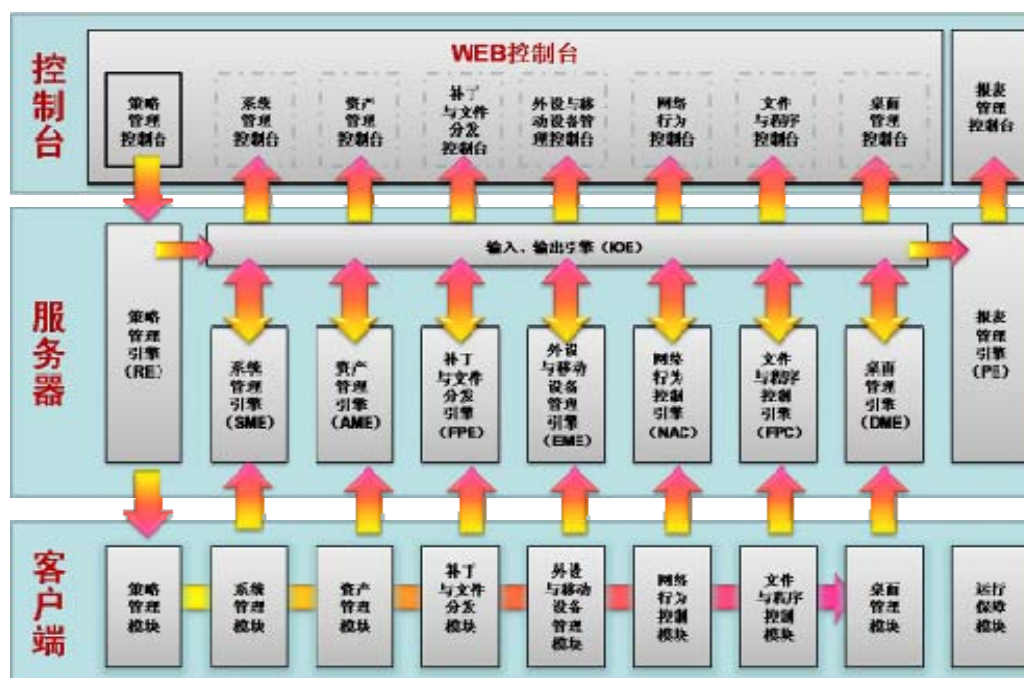


## 产品四 亚略特终端与内网安全管理系统

亚略特终端与内网安全管理系统可以对内部终端计算机进行集中的安全保护、监控、审计和管理，可自动向终端计算机分发系统补丁，防止重要信息通过外设和端口泄漏，防止终端计算机非法外联，防范非法设备接入内网，有效地管理终端资产等。亚略特终端与内网安全管理系统可以与防火墙、漏洞扫描设备进行有机联动，共同提供全网安全解决方案。

亚略特终端与内网安全管理系统由终端管理、堡垒主机、亚略特集中身份管理系统这三个方案构成，可以单独使用、满足终端管理或服务器管理、应用管理的需要，也可以协同使用，满足全网统一管理的需要。

### 1、系统架构图说明



**控制台：**是对服务器进行操作的控制界面，用于监控每台安装有客户端的终端计算机，制定安全策略，下达对终端计算机的监控指令等。

**服务器：**用于管理终端计算机的资产和系统信息、漏洞补丁数据、所应用的安全策略等，并向终端计算机的客户端发送监控指令等。

**客户端：**安装在每台被管理的终端计算机上，用于收集终端计算机的信息，执行来自服务器模块的指令，完成对终端计算机的监控等。

## 2、系统功能特点

亚略特终端与内网安全管理系统可以对客户端的防病毒软件的安装、运行及病毒库升级与否进行管理，可以对用户的文件、进程、上网行为等进行管理，可以对客户端计算机上的文件、应用程序、上网行为等进行详细的审计。

### 基础功能：

- 策略管理
- 通讯管理
- 日志功能
- 基于分组的策略管理
- 角色与权限管理
- 查询与报表

### 主要功能：

- 准入控制管理
- 补丁分发管理
- 终端维护管理
- 上网行为管理
- IT 资产管理
- 信息访问控制
- 其他系统支撑功能

## 3、终端与内网安全管理系统登陆界面



## 产品五 指纹单机防护：亚略特指纹电脑安全卫士

### 1、应用背景

根据《涉及国家秘密的信息系统分级保护管理办法》、《涉及国家秘密的信息系统终端安全与文件保护产品技术要求》等国家保密规范标准，面向党政机关、军队、大型企事业单位等高保密需求专门研发，用于强化部署涉密计算机“指纹身份认证、指纹电子文件保险柜、指纹访问控制、指纹数据加密、指纹日志审计”，基于指纹生物特征“人证合一”的独到优势，全面提升涉密计算机系统抗攻击能力，落实涉密计算机“进不来、看不到、拿不走、读不懂、逃不脱”六强防护。

#### 安全卫士六强防护：

**进不来** 非法用户无法进入涉密计算机

**看不到** 非法用户禁止读取涉密文件

**读不懂** 非法用户无法识别涉密文件

**拿不走** 非法用户无法盗取涉密文件

**逃不脱** 指纹人证合一责任不可抵赖

**毁不掉** 非法用户禁止删改涉密文件

### 2、指纹电脑安全卫士选型介绍

#### 产品特点：

- 支持 Windows、Linux 操作系统
- 采用全球最小指纹芯片
- 活体识别，杜绝假冒手指
- 支持 1: 1、1: N 指纹比对模式
- 采用亚略特 Bione 动态优化算法
- 反跟踪、反编译处理

#### 产品功能：

- 指纹登陆电脑
- 指纹加密文件
- 指纹锁定程序
- 指纹密码托管
- 指纹电子文件保险柜
- 指纹日志审计

#### 产品选型：



TRM- I 型指纹仪



TRM-II 型指纹鼠标



FRT600 按压式指纹仪

## 产品六 亚略特基于指纹识别的终端安全登陆系统

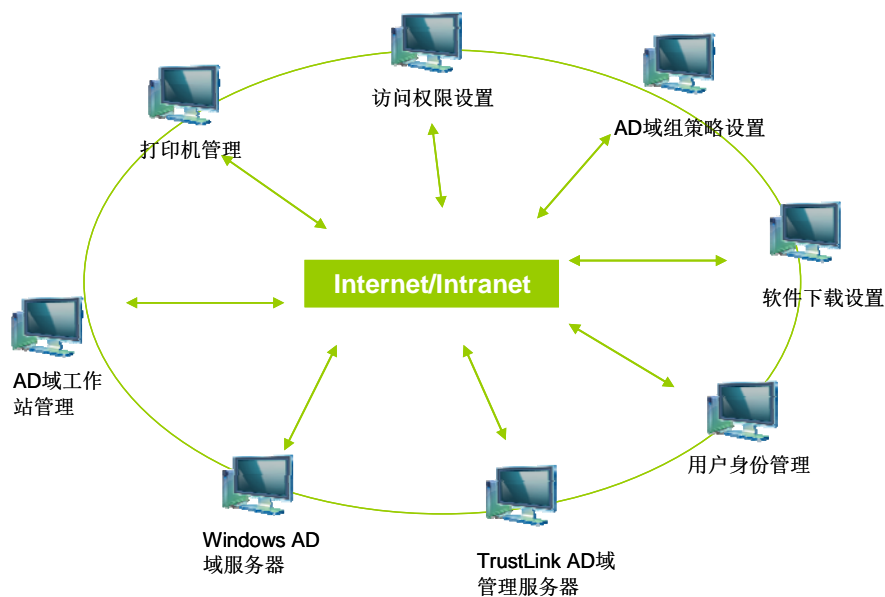
### 1、应用背景

亚略特基于指纹识别的终端安全登陆系统，又称指纹 AD 域用户身份安全管理系统是专门针对国内政府、军队、涉密科研所安全管理特点，以国家保密局《涉及国家秘密的信息系统分级保护技术要求》、公安部《计算机信息系统等级保护技术要求》为标准进行设计并研发的身份安全管理系统。

系统紧密结合 AD 域用户安全管理策略，以生物特征识别技术为手段，全面解决机构系统用户口令管理、安全使用等系列问题，采用先进架构设计，确保系统稳定安全、性能卓越。

亚略特 AD 域管理系统是目前国内唯一一家全面通过国家军队、国家保密局、公安部的权威认证的产品，已广泛应用于海军、空军、二炮等机要单位。

### 2、系统价值



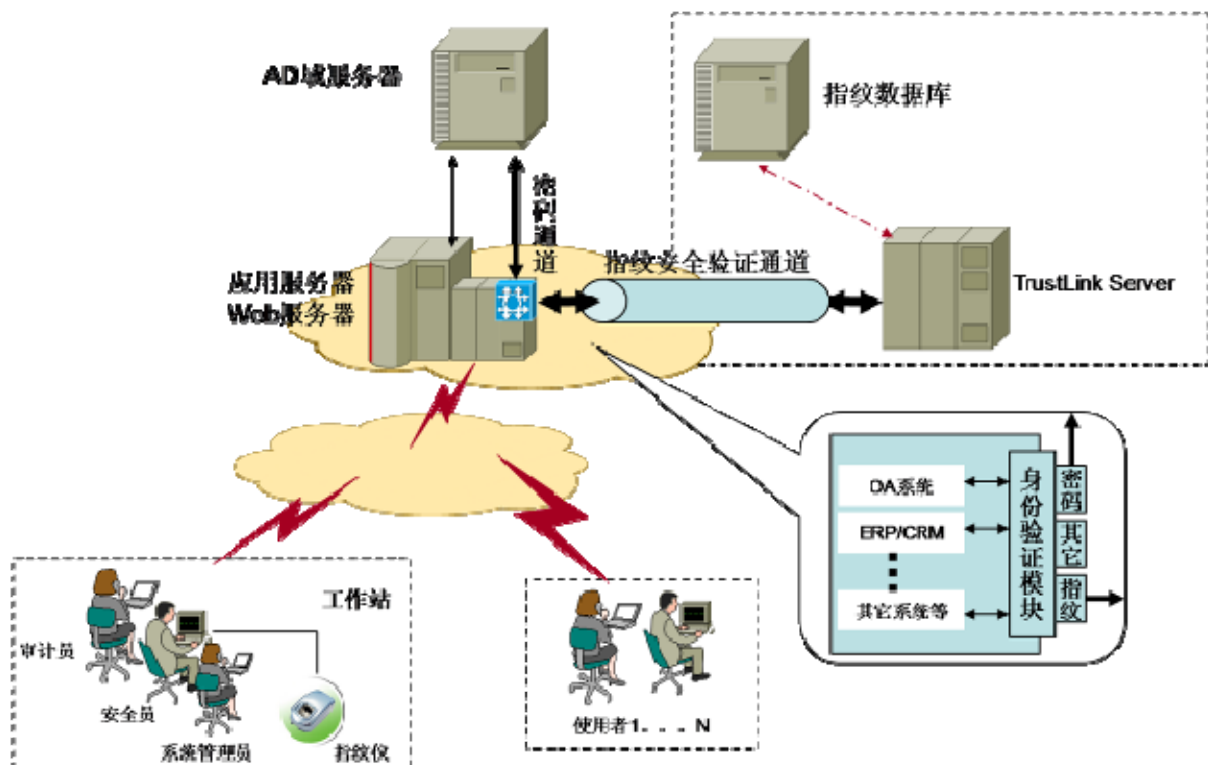
- 严格身份权限控制，基于指纹认证机制，实现访问权限及授权的精确控制，保护数据安全。
- 简化登陆认证环节，省去键盘输入密码的麻烦，优化用户验证体验。
- 降低 IT 维护成本，完全免去密码重置工作，解放 IT 维护生产力。
- 提升网络内控效益，基于指纹认证，确保身份、权限部署与实际安全策略全面一致，解决安全管理问题。
- 统一集中管理域系统中大批量用户身份的可信审计、系统登陆、权限访问。
- Web 化的域管理，AD 域与 Trustlink 服务器可实现同步信息传输、信息协调管理。
- 开放性的接入设计，支持不同终端设备验证。



### 3、系统功能特点

- 该系统是目前国内唯一一家全面通过军密、国密、公安部信息安全产品权威认证的产品。
- 平台化、网络化的指纹身份认证技术，安全可靠，可能根据安全需要实现多因子身份认证。
- 管理员、审计员、保密员“三员分离”管理。
- 采用 JAVA 技术的 B/S 架构 AD 域用户身份管理方式，可随时随地对域用户进行集中的管理。
- 指纹库、指纹比对、WebService 分布式网络架构部署。
- 支持最广泛的指纹认证采集终端接入。
- 用户可根据不同密级设置多指认证，确保各密级信息的安全性。
- 专用 Key 加密设计，防止指纹数据库泄漏。
- 指纹传输加密机制。
- 一次一密，动态密码策略。
- 系统的认证服务记录，实行日志安全审计管理。
- 指纹特征值 ID 号唯一性加密设置，防止后台非法篡改，确保指纹特征值存储安全。

### 4、指纹AD域系统网络结构图





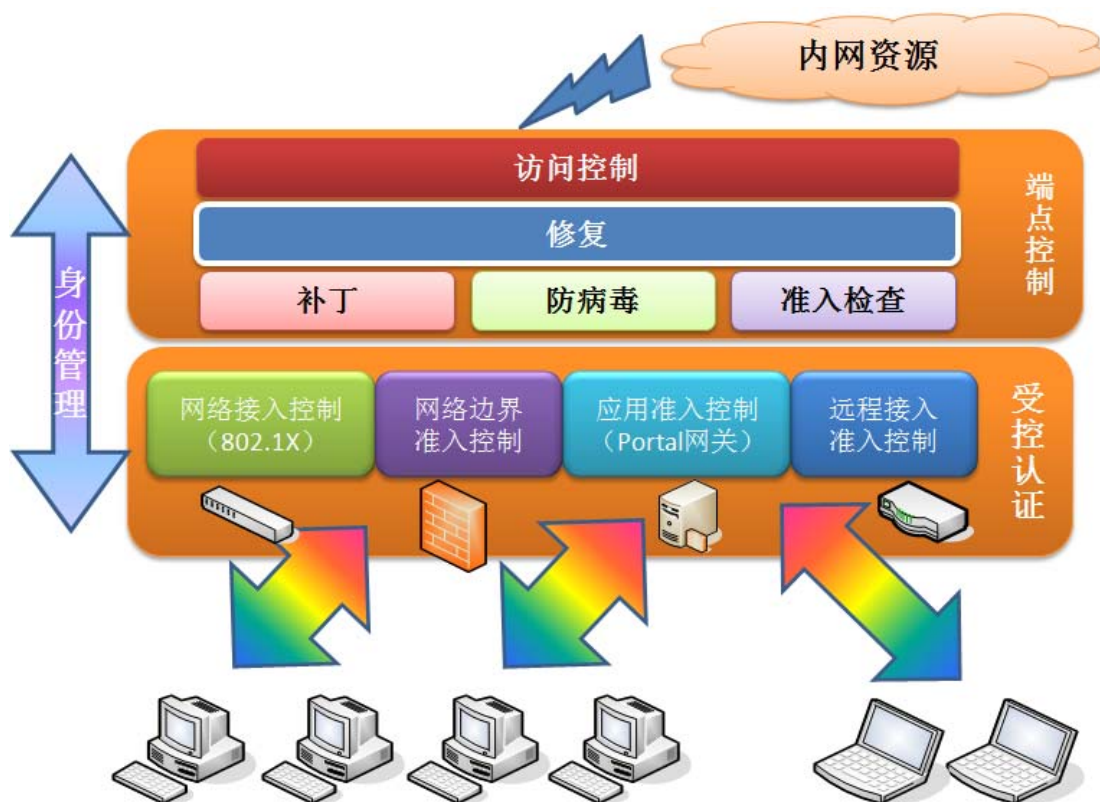
## 第三篇 安全接入管理指纹识别解决方案

### 系统背景

随着信息系统在政务、大中型企业实际应用过程中不断深入推进，各种业务审核、资源共享、信息发布，都交由应用系统来处理，而以虚拟化、VPN、SSO 等为主的 IT 接入技术则能满足分支机构、移动用户、合作伙伴快速实现信息交互，同时也产生了新的网络安全弱点。

比如，内部网络接入公网时的安全问题如何确保？SQL 蠕虫、“冲击波”、“熊猫烧香”等病毒与黑客通过网络接入的间隙连续性的攻击；口令泄密、硬件资产丢失、身份盗用等诸多网络接入时的不确定性安全问题，令政府机关和企业单位 IT 管理人员防不胜防，内部网络 IT 资产面临极大的安全威胁。

按照等级保护设计要求，内部网络接入公网要做好边界防护，而网络接入控制指纹识别方案，可以保护整个企业内部网络，包括可管理的（台式机、笔记本电脑、服务器）以及不可管理的（外部访客、合作伙伴、客户）终端，阻止未授权用户使用 IT 接入通道，在“入口”处维持接入途径的正常秩序，从而进一步维护传送数据的安全，防止对网络资产或私有信息的非法访问，使网络安全得到有效提升。



## 产品七 亚略特虚拟化身份安全指纹认证系统

### 1、虚拟化应用面临的诸多安全挑战

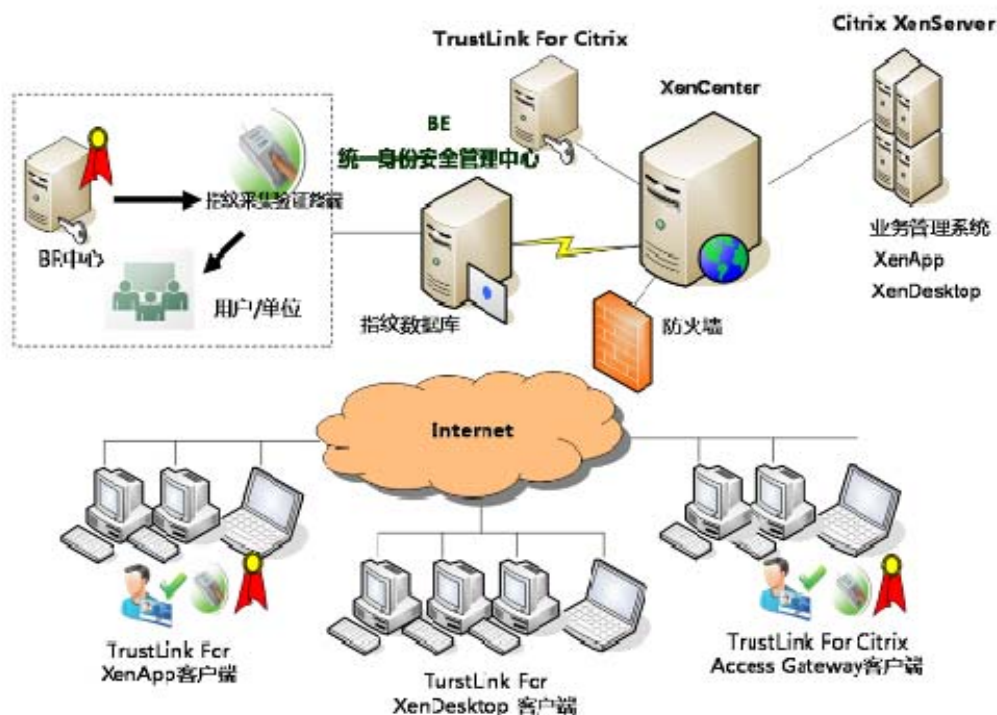
- 虚拟化访问用户的真实身份不能确定，安全策略无法被严格执行
- 虚拟桌面系统使用 username、password 方式认证，不安全
- 多个虚拟系统使用同一个账号及密码，身份易被冒用、共用
- 为了安全性的需要定期修改复杂的密码
- 虚拟应用使得很多终端硬件设备无法识别
- 多个应用系统如何做到登陆的安全与便捷相结合

.....

### 2、指纹虚拟化身份安全系统介绍

指纹虚拟化身份安全系统（Trustlink for Citrix）是指将亚略特指纹身份认证技术无缝集成到 Citrix 虚拟桌面，借助最安全可靠的生物识别身份认证手段，取代传统的“用户名+密码”认证模式，降低因身份冒用、共用等非法进入内网虚拟化桌面窃取机密资料的风险。同时，通过指纹识别强身份鉴别机制，提高应用虚拟化接入的安全性能，确保系统安全策略被严格执行，改善用户的网络接入体验，净化设备运行环境。

### 3、指纹虚拟化身份安全系统网络部署架构图

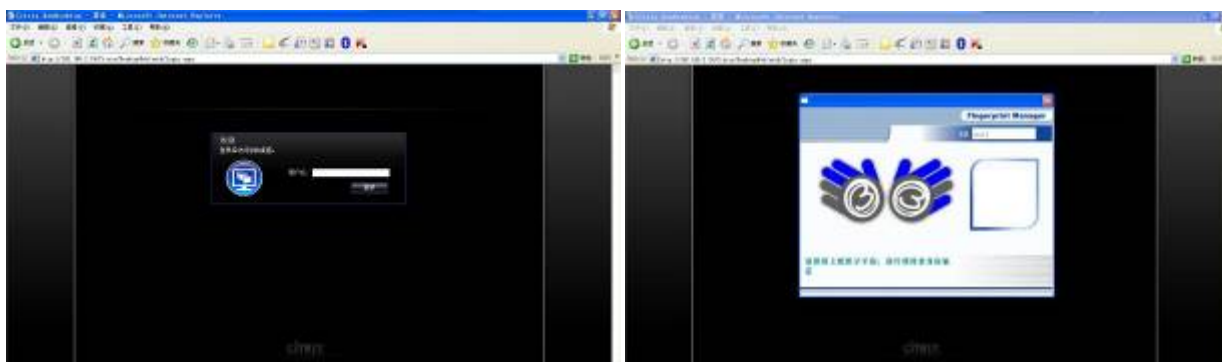


## 4、指纹虚拟化身份安全系统特点

- 建立集中统一的身份认证系统
- 多虚拟桌面系统使用统一身份认证 ID
- 多虚拟桌面系统使用统一认证方式
- 多应用系统使用统一身份认证 ID
- 多应用系统使用统一认证方式
- 对用户身份进行集中统一管理（人证管理、人机管理）
- 采用指纹识别方式进行高安全身份认证，人证合一
- 基于指纹识别硬件设备的硬件虚拟重定向

## 5、指纹登陆虚拟化的两种方式

### A、TrustLink For Citrix WebInterface 基于 Web 浏览器方式登陆虚拟化应用界面



### B、TrustLink For Citrix XenDesktop 基于瘦客户端方式登陆虚拟化应用界面

Step1:

瘦客户机指纹识别登陆

Step2:

无延时自启动虚拟桌面系统，虚拟系统用户身份与 AD 域用户身份实时同步

Step3:

虚拟系统验证域用户系统

Step4:

成功登陆



## 产品八 亚略特指纹SSL VPN远程访问系统

### 1、指纹SSL VPN系统介绍

传统 VPN 的身份认证方式通常是密码式认证、PIN 码认证、USBKEY 认证、短信认证等，指纹识别认证因其唯一性、不可替代性等优势已逐渐成为 VPN 身份认证的主流形式。

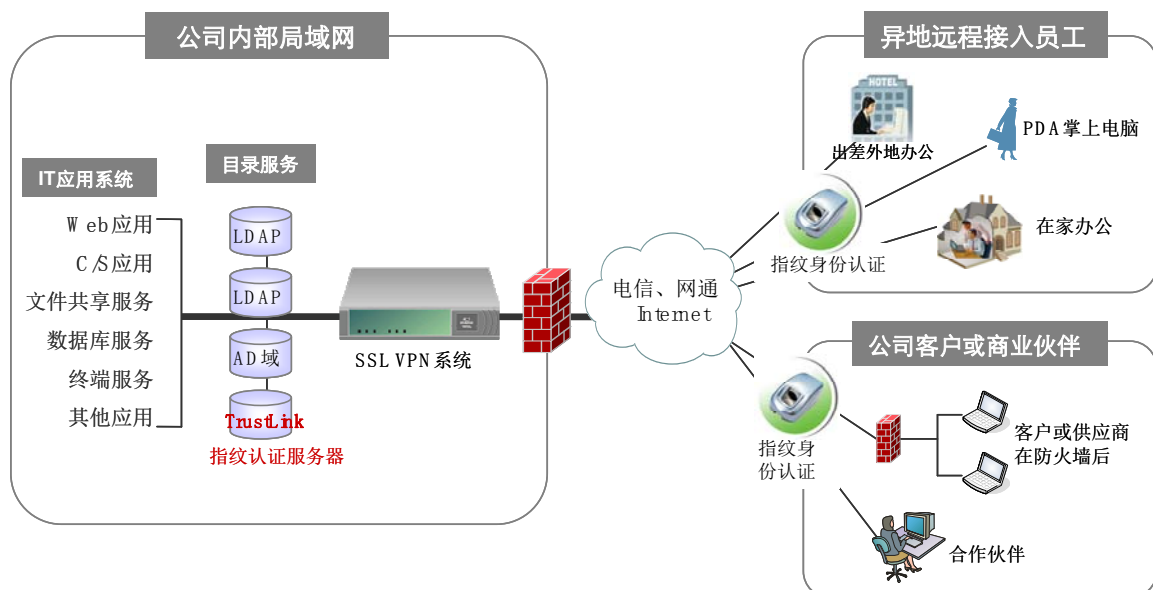
亚略特 TrustLink 指纹身份认证平台，提供指纹 WebService 集成接口，能与 VPN 系统无缝接入，将传统的口令认证模式，升级到指纹识别认证，将身份辨别落实到真实具体的用户本身，避免身份被盗用、共用等风险。

Trustlink 指纹认证服务器采用指纹登陆 SSL VPN 系统，对登陆的每一个用户进行权限管理和身份认证，对企业员工、公司客户、合作伙伴访问登陆实施安全日志审计，对专用网上的文件共享服务、应用系统数据库查询等 IT 服务按权限级别分开管理，确保企业网络远程访问的真实性与安全性，避免组织内部出现越权访问现象，专网上核心数据被非法用户窥视、窃取。

### 2、指纹SSL VPN系统价值

- 访问支持多元化，任何角色的员工通过指纹识别可登陆企业授信的网络资源。
- 建立安全日志审计，使专网信息访问操作有据可查，避免问责无果。
- 采用网络传输签名认证机制，所有传输的信息均经过签名加密处理，只有透过本人的指纹身份确认，才能进行合法认证服务，避免 VPN 专用网络传输时被篡改或其他不当操作。
- 指纹识别贯穿 VPN 虚拟专用网的每一个子业务系统的身份认证，即使用户登入专用网，进入各个业务系统仍可选择指纹验证身份，以确保访问用户从一而终的身份安全。

### 3、指纹SSL VPN系统网络架构图





## 产品九 亚略特指纹单点登陆管理系统

### 1、指纹单点登陆系统介绍

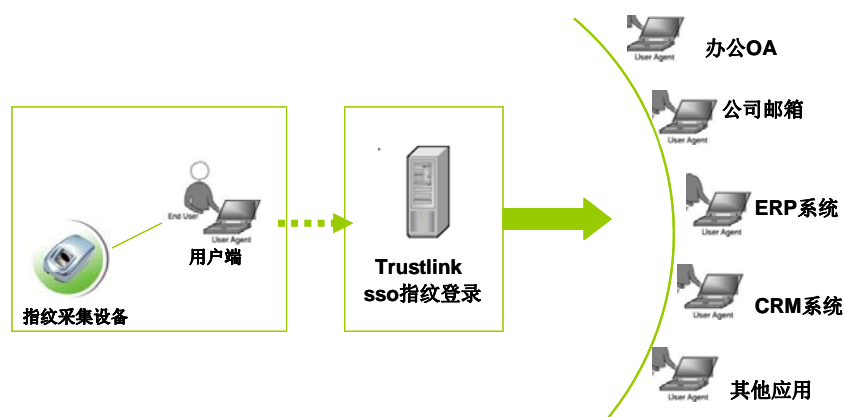
Single Sign-On，即单点登录，是指用户在一处登录后完成身份验证，即可访问其他所有相互信任的应用系统，而不需要再次认证。

亚略特指纹 SSO 单点登陆身份认证系统，与 TrustLink 指纹认证平台绑定部署，将指纹识别全面导入 IT 业务系统，实现指纹登陆、权限管理、用户身份辨别等功能，从用户终端进行指纹防护、网络接入指纹身份认证、有效提升网络系统 IT 内控强度，减少人为引发的管理风险。

### 2、指纹单点登陆系统价值

- 人证合一的指纹可信审计解决信息不可篡改、不可抵赖风险，规范用户信息管理，杜绝人为漏洞。
- 用户只在一处登录完成身份验证，即可互信访问其他所有相关联的业务系统。
- 显著降低 IT 密码维护成本，减少因密码遗忘、丢失、被窃等泄密风险。
- 统一的、基于角色的和个性化的信息访问，提高信息系统的易用性、安全性、稳定性。
- 适用于 Windows NT/2000/XP/2003，支持接入不同的指纹认证终端。

### 3、指纹单点登陆系统功能特点



**指纹管理：**配合指纹终端，对注册、删除、修改指纹库，进行统一管理。

**设备认证：**结合设备授权发放程序，通过指纹认证，确保授权用户与系统用户一致。

**统一资源访问入口：**经由指纹对企业内部相关联业务系统进行统一访问，相互切换。

**指纹比对：**实现客户端指纹采集与服务器站指纹身份快速比对，精确验证。

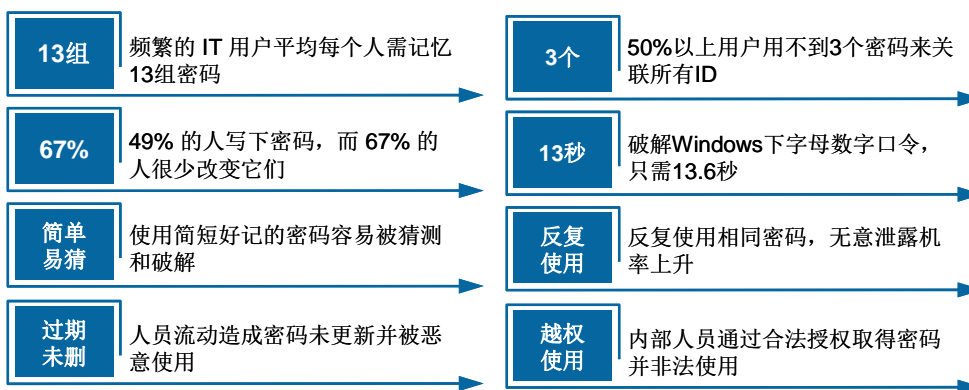
## 第四篇 身份鉴别管理指纹识别解决方案

### 系统背景

在政府和大中型企事业单位，各种业务审核、资源共享、信息发布，都交由应用系统来处理，如 OA 办公自动化管理系统、ERP 系统、CRM 客户关系管理系统、报税系统、档案管理系统、网上银行系统等。

有系统存在的地方，就有信息的安全管理问题，登陆用户身份识别与权限控制是网络安全管理的关键环节。然而，长期以来被人们所忽视，IT 管理者往往集中于一般安全防范，如：防火墙、入侵检测、防病毒等。事实上，最新的安全报告显示：在政府和大中型企事业单位的关键应用系统中，80%的安全问题发生在内部，而不是外部，内网安全问题可能是目前信息安全管理最脆弱的一环。

传统的“用户名+密码”是目前应用系统非常普遍的身份验证形式



由图来看，内网用户遭非法冒用、用户密码丢失已是非常普遍的现象。以指纹替代“用户名+密码”的形式，则能很好的提高 IT 风险抵御能力，实现指纹 OA、指纹 ERP、指纹 SSO 单点登陆、指纹财务系统等多种应用，将 IT 流程全面贯穿指纹识别机制，将传统管理中的权、责落实到 IT 中的真实身份，并提供基于指纹识别的内控日志审计，全面巩固内部网络的安全体系。

类别	应用特点	安全	方便	执行力★
帐号密码	物证分离	★	★★	★
IC卡	物品本身成为授信凭证，一经转让、混用、丢失即可导致权限置换。	★★	★	★★
动态口令		★★	★	★★
USB KEY	需要携带(或记忆) 使用繁琐 容易丢失 可能被盗	★★	★	★★
生物识别	人证合一			
	权利人与行使人时刻统一，管理执行严密无缝。	★★★★	★★★★	★★★★
	不需携带(或记忆) 不繁琐 不丢失 不可盗			



## 产品十 TrustLink 指纹身份认证平台

### 1、TrustLink平台介绍

中国第一个通过公安部销售许可认证的生物识别网络安全平台 — 亚略特 TrustLink 指纹识别身份认证平台，用于与第三方 IT 系统、应用软件无缝集成，将传统的“用户名+密码”身份认证升级为指纹识别模式，有效解决网络身份冒用、共用、盗用等问题，巩固 IT 系统身份安全、IT 内控管理安全，优化用户认证体验，提升服务效率。

该平台是基于公安部“信息安全等级保护技术标准”，针对目前各单位网络办公自动化系统不具备完善的、符合国家有关等级保护要求的安全规则，无法用技术手段对分等级保护信息进行有效监管的实际情况，研发的独立身份鉴别系统，完全符合国家等级保护的相关要求。



### 创新的指纹识别集成模式

- 无须开发 1 天集成，具备每秒处理上万次指纹数据比对能力
- 分布式架构，支持各种主流数据库、开发语言
- 指纹系统与主应用程序相互独立，不形成系统依赖
- 支持接入全球主流指纹芯片 10 种以上
- 支持多种指纹认证终端
- 开发商无需对指纹系统进行开发、维护

### 引擎中国指纹 IT 应用市场

- 通过国家公安部信息安全产品权威认证
- 整合指纹 SS0、指纹 OA 等应用模式超过 30 余种
- 成功承建国家级百万人口指纹库
- 全球 ISV 合作伙伴超过 1000 家
- 全球最终用户超过 100 万



TrustLin 指纹认证界面

## 2、TrustLink指纹身份认证平台功能

### • 身份鉴别子系统

用户使用系统，首先必须通过客户端登录并进行身份鉴别。具有指纹身份注册、指纹比对、指纹修改等指纹管理功能，通过指纹特征值来作为各项应用系统登录与各项操作确认的身份控制。

### • 转授权访问控制子系统

系统采用强制访问控制策略。系统仅授权系统管理员对转授权访问控制规则进行设置,并将设置信息生成日志记录,同时对控制规则生成备份。人员的权限由系统管理员设置，经系统安全员审核通过后才能生效。

### • 安全审计子系统

系统对审计身份鉴别事件按安全等级分类为一级报警、二级报警和三级报警。审计管理员重点审查一级报警和二级报警日志信息。

### • 标准对外接口

对外接口包括身份认证接口、访问控制接口和安全审计接口，采用 COM 组件和 EJB 组件技术来实现。提供简单灵活、功能强大的对外接口，简化了与其他业务系统的衔接工作，大大提高了其他业务系统的安全保密性。



TrustLink 指纹身份认证平台 用户管理界面

### 3、TrustLink 指纹身份认证平台特点

#### (1) 五种安全防范机制

- 指纹加密传输签名机制

网络传输的指纹信息均受加密保护，指纹在传输过程中被加载一次性密钥及时间戳，只认证合法的指纹身份，避免网络传输时被篡改及不当使用。

- 时间戳机制

指纹认证服务器在被要求进行识别服务时，所有传输资料将被加载时间戳，若在有效时间内未传回则视为异常，系统拒绝服务。

- 指纹特征值存储安全机制

Trustlink 将所有指纹资料与指纹比对模板分开储存，系统不保存指纹特征值模板，而是保存加密处理后的密钥模板，确保密钥随机产生且一次有效，实现安全的指纹认证。

- 容错备份机制

提供主服务器无法运作时资料及系统容错备份机制，确保系统持续顺畅运作，不因单一主机出错而中断重要工作。

- 负载均衡机制

提供在同一时间内大量认证资料需求之平衡负载机制，以达到流量分担的功能，避免发生系统单点故障状况。

#### (2) 灵活的平台扩展能力

- 支持全球主流芯片：Authentec、UPEK、Digitalpersona、LTT、Validity、Atrua、FPC 等。
- 支持多种应用架构：C/S、B/S、N-Tier。
- 支持多种数据库：Access、MS Sql Server、Oracle、SyBase、DB2、MySQL 等。
- 支持多种开发语言：VB、PB、Delphi、VC++、ASP、JSP、Java、.Net 等。
- 支持多种生物识别认证：脸型、虹膜、声音、脸形等。
- 支持多种指纹认证终端：支持亚略特全线指纹产品。
- 支持百万级人口指纹库验证能力：亚略特 1: N 运算引擎，具备百万级人口指纹库验证能力。

#### (3) 完善的安全策略

- 防指纹数据库泄漏

Trustlink 将用于管理指纹数据库的 Key 进行特别加密，只有系统管理员知道，即使数据库被攻

破，没有 Key 解密，指纹特征模板仍然无效。

- **多指身份认证**

可一性注册多枚指纹，UI 显示注册手指，用户可根据不同密级设置多指认证，确保各密级信息的安全性。

- **分布式网络部署架构**

指纹库、指纹比对、WebService 服务器可分别部署于不同服务器中，减少因系统过度紧密结合引发服务器系统不稳定的可能，采用安全备份策略，确保指纹存储安全，Trustlink WebService 技术，零障碍穿透防火墙。

- **安全日志审计**

系统的认证服务记录将被记载到数据库日志中供管理人员进行安全核查，实现日志的可配置管理，双机热备的相关资料日志。

- **帐号自动保护**

若用户指纹在认证过程中发生连续错误，则该用户帐号将自动被锁定，以此加强用户身份验证的安全管理。

- **生物识别智能搜索引擎**

提供支持多层级主机认证，适用于各种层级的主机配置架构，加快资料搜索速度，提升系统整体效能。

#### **(4) 安全便捷的后台管理**

- **指纹集中统一管理**

人机交互式的后台管理，指纹注册、比对、修改、删除、注销等指纹管理，即用即会。

- **黑名单设置防身份篡改**

Trustlink 独创的指纹黑名单功能，备份已比对的指纹特征值，防止人为篡改导致丢同样的特征值非法访问，防身份假冒、身份复制、比对数据截取。

- **指纹权限冻结**

员工离职，或是员工权限暂时终止，管理员可第一时间冻结用户指纹阻止系统访问，不需要删除数据库中的指纹。

- **实时监控**

指纹认证服务器 24 小时实时监控系统的各应用服务器、运行环境、数据库服务器，一但有黑客攻击，即自动报警。

#### **(5) 超强的组件化设计能力**

针对目前普遍应用的 Windows 平台提供的 ActiveX 及 DLL 组件，在非 Windows 平台下应



用时，TrustLink 则提供标准的 JAR 文件供其跨平台应用，其中的大量 CLASS 可方便的让 JAVA 开发者调用，不需改变原有体系架构，节省用户的开发成本、时间成本。

#### 4、TrustLink Web Service 网络指纹认证管理

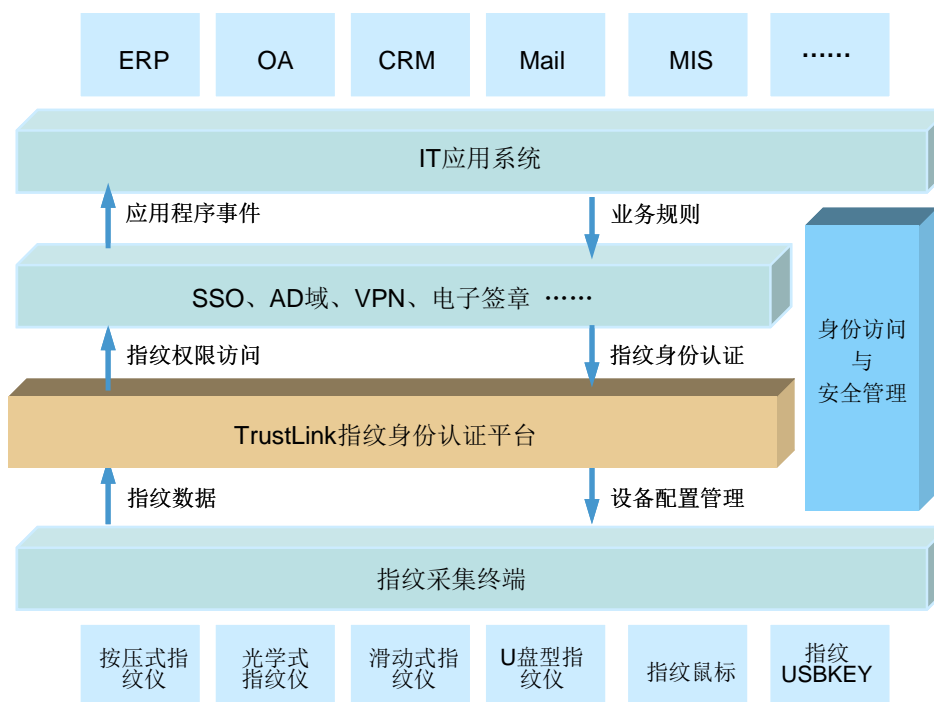
##### 什么是 Web Service ？

Web Service 是建立可互操作的分布式应用程序的平台，是一个用于分散和分布式环境下网络信息交换的基于 XML 的通讯协议，它通过一系列标准和协议来保证程序之间的动态连接，为各种开发语言提供统一访问标准，使原来各个孤立站点之间的信息能够相互通信、共享，使各级应用系统之间能相互流通，相互访问，使应用程序能被更广泛的用户访问。

##### 什么是 TrustLink Web Service ？

在实际应用过程中，各个系统因开发语言(如 VB、java、.net 等)的接入端口、变量定义不同，容易造成不同开发语言的系统之间无法相互共享、兼容整合。此外，Web Service 是在 Internet 开放性的环境下公开部署的，对组织内部网络环境存在很大的安全隐患。

亚略特 TrustLink Web Service 网络身份认证管理，遵循 HTTP、TCP/IP 协议的 Web 化架构，基于 Web Service 的技术服务，并向用户提供统一标准的应用服务接口，不受局域网限制，可直接穿越防火墙，为组织内部网络提供“真实”的身份认证访问，巩固内网安全体系，优化用户身份验证体验，提升 IT 系统风险抵御能力。



TrustLink 指纹身份认证平台应用拓扑图

## 产品十一 亚略特指纹数字签名身份安全管理

### 1、传统PKI应用背景

目前我国电子签名市场通行的是数字签名技术，也就是 PKI(public-key infrastructure)，公共密钥加密，USBKEY 则作为支持 PKI 应用的基本硬件配置，成为保护客户数字证书和私有密钥的安全载体。

传统 PKI 应用是客户认证端通过 USBKEY 保护私钥，然而基于 PIN 码的保护手段存有隐患，即使数字证书是合法的，PIN 码认证的却是口令，并非真正的授权用户，黑客获得口令即可进行合法操作。其次，服务器认证通过后，PKI 通道正式建立，用户即可进入权限的批量操作环节，过程当中无须再次认证，万一中途离开，则存在被他人误操作、恶意操作的风险。

将指纹识别引入数字签名机制，以指纹取代 PIN 码，保护数字证书在 USBKEY 硬件内部完成指纹识别身份保护，保证用户每一次权限操作仍需要指纹认证，以保障每一次数字签名都合法可靠。而且，在万一用户遗失 USBKEY，来不及冻结数字证书的情况下，服务机构也可在第一时间冻结用户指纹信息，即便数字证书外泄，也能及时有效地保护用户身份和相关权限。





## 2、亚略特指纹USBKEY产品介绍

亚略特 FPK300 指纹 USBKEY，采用亚略特领先的指纹硬件技术，形成新一代“指纹数字签名”USBKEY 安全设备，具有运算频率高、速度快、卓越片内指纹算法、优越性价比等优势。

FPK300 提供标准接口，不仅符合 PKI 体系，可同时用于数字签名指纹身份认证、网络身份指纹认证，整合“指纹登陆、指纹身份管理、指纹权限管理”功能，一 Key 多用，为更多 IT 系统，如 OA、CRM、财务系统提供指纹身份安全认证服务，为电子商务、电子政务等行业提供多重指纹安全防护应用。



型号： FPK300

## 3、功能特点

- 通过国家公安部信息安全产品销售许可认证。
- 指纹结合数字证书，数字签名，数据加解密更安全。
- 指纹替代 PIN 码，无需记忆，安全易用。
- 指纹注册、验证识别在安全芯片内完成，安全可靠。
- 高速 SoC 安全处理芯片，带硬件随机数发生器。
- 亚略特 Bione 指纹动态优化算法，高效快捷。
- 提供标准接口，满足全方位的 PKI 应用。
- 提供 SDK 开发工具包，支持 X.509 V3 标准的数字证书应用。
- 符合 CE 和 FCC、PKCS #11 / MS CAPI 规范。
- 无缝接入 TrustLink，提供 IT 系统身份安全认证服务。
- 即插即用，无需安装，指纹程序自动运行。
- 指纹数字签名，提升传统 PKI 体系安全。
- 结合设备授权发放程序，通过指纹认证，确保授权用户与系统用户一致。

## 4、应用领域

- 电子商务交易认证终端
- 电子政务电子签名认证终端
- 面向 PKI 软件开发商、系统集成商数字签名指纹认证解决方案

## TrustLink 指纹采集终端选型指南

产品型号/名称	产品图片	比对模式	适用范围
TL-FR0460 光学按压式指纹仪		1: 1/1: N	适用于中小型指纹库身份认证终端
TL-FR0500 光学按压式指纹仪		1: 1/1: N	适用于百万级大型指纹库身份认证终端
TL-FRS121 滑动式指纹采集仪		1: 1	适用于保密单位、科研机构等信息安全身份认证终端
TL-FKS180 滑动式 U 盘型指纹 签名仪		1: 1/1: N	适用于政府、大中型企业身份安全终端 含 1G 指纹安全存储空间
TL-FPK300 指纹 USBKEY		1: 1/1: N	适用于政府、大中型企业身份安全终端 支持 PKI、指纹识别技术整合应用，提供 SDK
TL-FRT600 电容按压式指纹仪		1: 1/1: N	适用于金融证券、商业机密、政府涉密等高端信息安全领域应用
TL-FRT610 电容按压式指纹仪		1: 1/1: N	适用于金融证券、商业机密、政府涉密等高端信息安全领域应用

\* 产品详细介绍资料，请咨询亚略特销售人员

## 第五篇 亚略特资质荣誉及典型案例

### 一、亚略特 资质荣誉证书



军密 U 盘认证证书



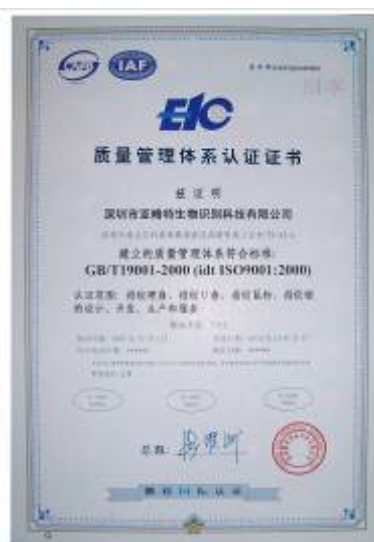
军密硬盘认证证书



国密认证证书



知识产权证书



国际 ISO 认证



亚略特终端与内网安全登  
陆国家保密局检测证书



商用密码定点生产单位



商用密码产品销售许可证书



软件企业认定证书



软件产品登记证书

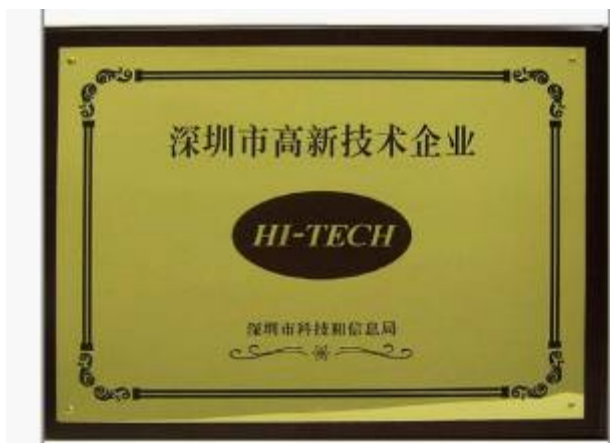


计算机软件著作权登记证书



公安部信息安全产品销售许可

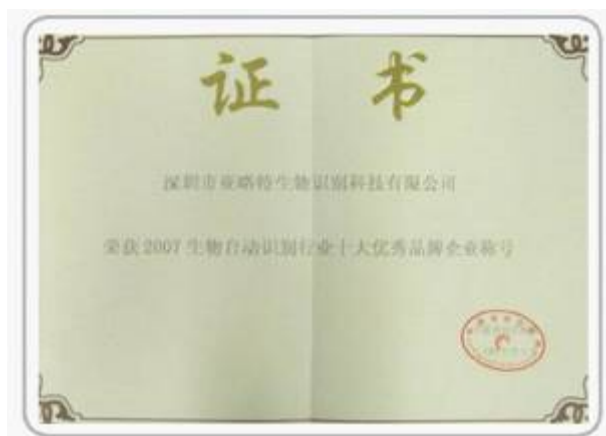




深圳高新技术企业



计算机防护优秀解决方案



生物识别十大品牌



自动识别系统集成十大品牌



优秀指纹平台软件产品奖



最值得信赖生物识别品牌



十大最具创新性技术奖



第 11 届高交会创新产品奖



2009 年度创新先进企业



2009 年信息安全优秀解决方案奖



## 二、亚略特 信息安全典型案例

### 1、政府单位典型案例

#### 客户名称：民政部

项目简介：全国流浪乞讨人员救助管理指纹认证系统

应用成果：建立流浪乞讨人员、特殊困难人员指纹数据库，对受助人进行精准甄别，高效防范“搭便车”等骗助行为，并为特殊困难人员寻亲遣返提供准确线索。同时，对系统管理加以指纹登陆控制，使公民信息得到重视和妥善保护，显著增强政府监管工作的有序化和透明度，提高政府的服务质量和职能效率。

#### 客户名称：国家卫生部

项目简介：全国社区医疗卫生指纹认证系统

应用成果：将方便快捷的指纹识别作为社区居民的身份认证手段，建立集中规范的“电子健康记录”，为社区卫生服务提供高质量的数据支撑。

#### 客户名称：国家保密局、江苏保密局、广东保密局、北京保密局、四川保密局、湖南保密局等

项目简介：涉密移动存储介质管理及指纹 OA 系统安全登录

应用成果：针对涉密存储介质存在容易泄密、泄密事件管理追踪困难等问题，在涉密移动存储介质管理等环节引入指纹识别技术，通过用指纹涉密 U 盘/指纹安全硬盘替代传统的普通 U 盘和硬盘，指纹 OA 登陆系统，确保用户身份的唯一，提升涉密安全等级，降低主动和被动泄密风险。

#### 客户名称：信息产业部

项目简介：国家计算机网络应急中心业务办公指纹身份认证系统

应用成果：隶属国家保密机构，在系统的登录、公文浏览、审核等环节采用了亚略特指纹识别身份认证系统，确保用户身份真实统一，系统“内外安全”的一致。

#### 客户名称：国家人事部

项目简介：OA（办公自动化）指纹认证系统

应用成果：针对政府 OA 办公自动化系统的使用过程中出现的身份安全问题，亚略特 OA（办公自动化）指纹认证系统，克服原有传统密码认证存在的不安全漏洞，更大的提高了 OA 系统的安全防范能力和实际工作效率。

#### 客户名称：公安部

项目简介：指纹经济侦查系统、涉密移动存储介质

应用成果：在国家公安部的经济侦查系统中，采用亚略特指纹识别技术，将指纹 USBKEY 联结到每个用户的登陆系统，并对系统访问权限进行控制，以确保经济侦查系统使用用户的真实身份统一，做到安全管理。

项目简介：全国驾驶员指纹比对系统

应用成果：驾驶员考试指纹比对系统，对驾驶员考试时做指纹身份确认，防止代考等违规的考试现象，有效的对驾驶员考试做规范化管理。

**客户名称：最高人民检察院**

项目简介：指纹涉密移动存储管理系统

应用成果：在存储机密文件和数据保护方面，采用指纹增强身份认证技术，做到在内网仅能使用安全区，公开区不可用；在外网仅能使用公开区，安全区不可用。

**客户名称：北京市检察院、浙江省检察院、四川省检察院、河南省检察院、陕西省检察院、新疆省检察院、内蒙古检察院**

项目简介：指纹涉密移动存储介质

应用成果：针对涉密存储介质存在容易泄密、泄密事件管理追踪困难等问题，在涉密移动存储介质管理等环节引入指纹技术，通过用指纹涉密 U 盘/指纹安全硬盘替代传统的普通 U 盘和硬盘，确保用户身份的唯一，提升涉密安全等级，降低主动和被动泄密风险。

**客户名称：深圳南山区检察院**

项目简介：指纹 SSO 单点登陆

应用成果：各种电子邮件系统、OA、公文流转、人事管理系统等在日常工作中广泛应用。指纹 SSO 单点登录，使用户在一处登录后完成指纹身份验证，即可访问其他所有相互信任的应用系统，而不需再次认证。

**客户名称：河北财政厅，四川甘孜州财政局，黑龙江财政厅**

项目简介：指纹认证国库支付系统

应用成果：采用指纹增强身份认证技术，有效的管理国库集中支付的人员身份确认问题，规范了财政款项申报、审批、发放的全过程，对整个国库集中支付系统做统一的规范化管理。

**客户名称：北京市委、浙江省委、高级人民法院、公安厅、卫生厅、安全厅**

项目简介：指纹涉密移动存储介质

应用成果：针对涉密存储介质存在容易泄密、泄密事件管理追踪困难等问题，在涉密移动存储介质管理等环节引入指纹技术，通过用指纹涉密 U 盘/指纹安全硬盘替代传统的普通 U 盘和硬盘，确保用户身份的唯一，提升涉密安全等级，降低主动和被动泄密风险。

**客户名称：山东政法委**

项目简介：指纹电子公文审批系统、涉密移动存储介质

应用成果：在电子公文审批工作时，通过TrustLink指纹认证平台，提供可信的指纹身份验证服务，解决用户身份通过信息化系统是否可信这一安全策略的核心问题。

**客户名称：四川都江堰**

项目简介：新农村医疗管理信息化指纹认证系统

应用成果：新农村医疗管理信息化指纹认证系统中，传统的表单电子病历管理方式，全部升级到与病人本人的指纹相关联。不仅普通农民患者享受到了“一指辨认，高效诊断”的新医疗服务，更大大节约了急诊、病危、无自知意识患者的就医诊断时间。

**客户名称：福建海事局**

项目简介：指纹海运危险品申报

应用成果：海关系统通过引入亚略特的指纹身份认证系统，可实现系统操作人员及报关员的网上身份验证和信息加密，使海关各项管理作业更规范、统一、透明。在海事管理系统中，采用指纹增强身份认证技术，确认海运危险品申报人员身份，为海事信息化提供了全新思路 and 成功典范。

**客户名称：四川西昌监狱**

项目简介：指纹监狱管理系统

应用成果：由亚略特公司自主研发监狱指纹管理系统，使狱政管理实时、高效、安全、严密又轻松自如，全面摆脱人盯人的传统模式，进入一个全新的高科技管理时代。

**客户名称：浙江省药监局**

项目简介：药品指纹管理系统

应用成果：对于处方药的管理，一直是目前药品管理的重大难题。药品指纹管理系统可以有效的管理各个药店对于处方药的销售，即处方药必须在该药店药剂师的指纹确认下方可销售。

**其他政府型客户：**

- 公安部出入境管理
- 公安部第二代公安数字证书（指纹 USBKEY）
- 公安部经侦管理系统
- 公安部驾驶员考试系统
- 高检网站内容发布指纹审核系统
- 上海静安区检察院
- 广东省育龄妇女管理指纹认证系统
- 民政部军人优抚管理指纹认证系统
- 无锡市医疗保险指纹认证系统
- 广东省社保业务系统指纹认证系统
- 内蒙古自治区国安厅
- 民政部农村村民选举指纹投票系统
- 大连住房公积金管理中心
- 国务院港澳办指纹 OA（等级保护）
- 国务院法制办指纹安全移动存储介质
- 贵州省组织部
- 哈尔滨市委组织部
- 山东省质检局
- 山东省青岛市安监局
- 内蒙古自治区海关
- 浙江省国安厅

## 2、军队信息安全典型案例

**客户名称：中国人民解放军海军总部**

项目简介：电子资源档案管理指纹身份认证系统

应用成果：在军事信息化管理系统的用户管理、系统登陆使用等环节引入指纹身份识别，确保用户身份的真实性和唯一性，并且将指纹加密硬盘用于重要军事信息的存储，确保数据安全。

**客户名称：中国人民解放军空军总部**

项目简介：安全移动存储器 I—II 型

应用成果：与空军机要所共同研发适合空军安全部门使用的移动存储设备-安全移动存储器 I—II 型。用于重要军事信息的存储，确保数据安全。

**客户名称：兰州军区、北京军区、南京军区、成都军区、新疆军区、广州军区、沈阳军区**

**亚略特为济南军区唯一指定涉密存储介质提供商**

项目简介：军用指纹涉密信息防护系统

应用成果：为了提高计算机涉密信息的安全防护能力及对指挥专网及军事综合信息网的涉密信息的存储、使用和管理做到增强安全防护，采用亚略特军用指纹涉密信息防护系统，从单机层、移动层到网络层做到整体架构的信息安全策略全面统一、确保数据安全。

**客户名称：武警总队**

项目简介：武警部队值勤信息系统

应用成果：保护客户端 PC 安全，同时完美结合武警机要部门 517 平台，使用户利用指纹身份认证平台进行网络数据传输、网络用户身份认证，确保用户身份真实安全可靠。此系统下设多个指纹认证平台，从总部到中队全部采用指纹识别认证方式，此系统为目前武警部队最大的安全管理系统。

**客户名称：中央警卫局、中央秘书局**

项目简介：指纹涉密移动存储介质

应用成果：为了提高涉密信息的存储、使用和管理做到增强安全防护，采用指纹增强身份认证要求，达到涉密存储介质的涉密安全要求。

**客户名称：总后勤部自动化局、总参管理保障部**

项目简介：指纹终端防护及涉密存储介质管理

应用成果：为了满足中国人民解放军总后勤部自动化局对移动存储介质安全管理的要求，亚略特落实具体需求，并提供 PC 终端防护+移动存储介质管理+涉密系统网络身份认证相结合的完整解决方案。

**客户名称：二炮部队研究院**

项目简介：指纹计算机及文件保护系统

应用成果：根据第二炮兵研究院某科研部的涉密要求，亚略特采用“计算机及文件保护系统”之一指纹涉密产品，对其研究成果进行一对一绑定，保护系统安全。同时对非法运行系统的相关执行文件进行指纹防护，达到涉密安全要求。

### 3、军工企业信息安全典型案例

**客户名称：胜利油田**

项目简介：指纹电子签章系统

应用成果：TrustLink 有效解决了“人章分离”状态下可能存在的“使用无序、管理失控”等危害，指纹电子签章，不仅比传统印章更方便，更安全，并且使用效率高，原则性更强。

**客户名称：中国宝安集团**

项目简介：指纹电子公文审批系统

应用成果：公文审批系统的可信度是目前急需解决的问题。采用指纹识别技术可以有效确认，在网络办公条件下审阅人（批阅人）的身份，从而避免因用户密码遗失或被盗用而引起的越权操作行为。

**客户名称：山西晋煤集团**

项目简介：指纹 OA、指纹电子签章

应用成果：晋煤集团引进 TrustLink 指纹电子签章系统，实现真实可信的 PKI 电子签名应用，并将 TrustLink 指纹认证功能导入已有应用系统，将网络业务系统的“用户名+密码”身份认证机制，普遍升级到指纹认证。

**客户名称：中国石化山西分公司**

项目简介：电子文件指纹防伪授权访问

应用成果：对系统中电子文件，不同级别的文件的查看，必须有特定的授权。指纹防伪授权访问即可实现对文件的授权访问，用户在系统中输入指纹确认身份后，即可对其拥有访问权限的电子文件进行访问。

**客户名称：东方汽轮机有限公司（简称东汽）**

项目简介：涉密电脑安全管理和涉密存储介质管理

应用成果：针对全厂涉密电脑，特别是涉密笔记本电脑，进行存储介质和电脑安全卫士双重保险套件配套，使科研技术产品等涉密信息严格把控。

**客户名称：中电十四所、十五所**

项目简介：涉密存储介质管理

应用成果：为了提高涉密信息的存储、使用和管理的安全级别，采用指纹涉密存储介质管理系统，增强安全防护，全面达到涉密存储介质的涉密安全要求。

**其他军工企业客户：**

- |                     |                 |                  |
|---------------------|-----------------|------------------|
| • 中国船舶重工集团三个研究所     | • 陕西航天六院        | • 5701 航天服装      |
| • 陕西飞机工业集团(182 厂)   | • 山西卫星测探基地      | • 四川二重集团         |
| • 华燕航空仪表有限公司（141 厂） | • 甘肃酒泉基地        | • 四川东方电气         |
| • 7105 长征机械厂        | • 中国电子科技集团 22 所 | • 航天风洞实验室        |
| • 7102 燎原机械厂        | • 中船重工研究所       | • 核动力院           |
| • 611 中国航天设计研究院     | • 昆明造船          | • 西南核物理研究院       |
| • 7111 烽火机械厂        | • 航天工业集团        | • 中国航天一院         |
| • 山西黄河厂             | • 624 涡轮机厂      | • 航天三院           |
| • 陕西 618 所          | • 5719 航天科工     | • 兵器 203 所、204 所 |





指纹信息安全专家



亚略特生物识别科技

**深圳市亚略特生物识别科技有限公司**

ShenZhen Aratek Biometrics Technology Co.,Ltd.

地址：深圳市南山区高新科技园南区软件园T2-A栋2楼

电话：0755-26719975 26018866

传真：0755-26719930

网址：[www.aratek.com.cn](http://www.aratek.com.cn)

**华东平台：无锡指网生物识别科技有限公司**

地址：无锡市锡山经济开发区新竹路2号搜客天地大厦1楼

电话：0510-88258890

传真：0510-88250077

网址：[www.biokee.com](http://www.biokee.com)