

mToken K9 （ 指纹 KEY ）

技术白皮书



北京世纪龙脉科技有限公司

Beijing Century Longmai Technology Co., Ltd.

All rights reserved

版权所有侵权必究

目 录

目 录	2
第一章 背景概述	4
1.1 项目背景	4
1.2 产品定位	5
1.3 目标群体	5
第二章 产品介绍	5
2.1 产品外观	5
2.2 产品性能	6
2.2.1 技术参数	6
2.2.2 产品特性	7
2.3 操作系统支持	7
2.4 浏览器支持	7
2.6 COS 特性	8
2.7 指纹与 PIN 管理模式	9
2.7.1 管理员 PIN 与管理员指纹	9
2.7.2 用户指纹	10
2.7.3 指纹创建	10
2.7.4 指纹删除	11

2.7.4 指纹解锁.....	11
2.8 中间件支持	12
2.9 典型应用	12
第三章 产品特点	13
4.1 指纹 KEY 特点	13
4.2 应用特点	13
4.3 浏览器支持列表	14
第四章 指纹 KEY 与普通 USBKEY 对比	15
第五章 联系我们	16
公司总部	16
杭州办事处	16
广州办事处	16
成都龙脉	16
申请试用	17
购买产品	17
技术支持	17

第一章 背景概述

1.1 项目背景

随着计算机互联网技术的发展，网上应用日益增加，人们对信息安全保护要求越来越高，传统的 USB KEY 已不能保障用户的安全，这给信息安全带来了新的挑战。根据《中华人民共和国信息安全等级保护管理办法》明确规定我国各级计算机信息系统须有用户身份鉴别功能，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）等特殊信息进行身份鉴别”，需要有两种以上的身份鉴别机制；依据《涉及国家秘密的信息系统分级保护技术要求》：“**身份认证方式应该使用指纹等强身份认证方式**”保密要求，以生物识别机制来安全鉴别身份，使用独一无二的『指纹』取代令人诟病的密码进行身份认证。指纹是重要的人体生物特征，具有人别鉴识之用，所以北京世纪龙脉科技自主创新研发指纹型身份认证产品 mToken K9。

mToken K9 将传统的 USBKEY 身份认证功能与指纹鉴别技术相结合，利用指纹鉴别身份的唯一性代替传统密码。mToken K9 存储人体『指纹』特征，每个用户的指纹存储在一个防篡改的智能卡中，在身份认证过程中需要鉴别活体指纹特征，避免用户在使用普通 USBKEY 时，设备遗失或密码泄露带来的安全隐患。为了加强用户信息保护，使用自己的生物特征对自己的身份实现认证，防止非授权用户的访问和非授权资源的使用，保证信息安全。

1.2 产品定位




针对客户需求，mToken K9 产品采用 32 位具有国密型号的安全芯片与指纹采集器结合，指纹特征技术与数字证书认证相结合而专门研发设计的一款达到较高安全性身份认证产品。mToken K9 使用方法与应用场景和传统 USBKEY 一样，具有传统 USBKEY 的安全性、标准性，又具备生物识别的唯一性和易用性，是一款集指纹识别算法、国密算法，数字证书等技术于一体的商密产品。

1.3 目标群体

- ✧ 政府信息化办公人群
- ✧ 大型企事业信息化办公人群
- ✧ 高端客户群，追求产品创新人群

第二章 产品介绍

2.1 产品外观

名称	外观		
K9	正面	侧面	铭牌
			

备注：可根据客户要求，订制外观、LOGO 丝印以及刻字。

2.2 产品性能

2.2.1 技术参数

USBKEY 参数	
项目	参数
供电方式	USB 口供电
工作电压	5V (USB 口供电)
工作电流	50mA
工作温度	0 - 70 摄氏度
存储温度	-20 - 85 摄氏度
通讯协议	USB Mass Storage/ HID /CCID
接口类型	USB2.0 , 兼容 USB 3.0 , USB1.1
处理器	32 位高性能智能卡芯片
内置安全算法	RSA(1024/2048) SM1,SM2,SM3,SM4,SSF33 DES, 3DES, AES128/192/256, SHA1/SHA256/SHA384/SHA512,
用户存储空间	128K
数据存储年限	室温下数据保存最少 10 年
指纹特性参数	
项目	参数
指纹模块类型	主动射频式传感器
指纹识别	“活体” 指纹识别
指纹芯片寿命	1 , 000 , 000 次以上
指纹验证方式	1 : 1

	1 : N	
拒真率	<0.01%	
认假率	<0.00003%	
识别时间	1 : 1 , <10 毫秒 1 : N , <1 秒	
处理速度	40 帧/秒	
存储指纹个数	管理员指纹	10 个指纹特征
	用户指纹	10 个指纹特征

2.2.2 产品特性

mToken K9 指纹 KEY 支持多平台，支持国密系列算法，支持多种安全算法和中间件集成，支持 RSA (1024,2048) /SM2 证书导入，无需任何密码记忆，随手即可认证。

2.3 操作系统支持

- Windows
- Linux
- MAC OS
- 国产操作系统
 - 中科方德
 - 中标麒麟
 - 其它

2.4 浏览器支持

- IE 浏览器,360 安全浏览器,百度浏览器，腾讯 TT 浏览器，猎豹浏览器，傲游浏览器
- Netscape 浏览器，Firefox 浏览器, Google Chrome 浏览器,Opera 浏览器

- Apple Safari 浏览器

备注：mToken K9 硬件产品配合“龙脉国密 KEY 证书综合应用插件”无需二次开发,可实现跨平台跨浏览器使用,详情参见《龙脉国密 KEY 证书综合应用插件技术白皮书 V1.0》

2.6 COS 特性

- 自主知识产权 COS
- 符合 ISO7816 规范
- 支持 DES, 3DES, AES128/192/256, SHA1/SHA256/SHA384/SHA512, RSA(1024/2048)
- 支持国密算法：SM1,SM2,SM3,SM4,SSF33
- 支持多应用、多容器、多证书
- 支持 X.509 v3 证书存储及证书导入
- 性能参数

特性	参数
多应用	支持多个应用 最大支持 8 个应用
多容器	支持 64 个容器
多证书	典型值: 大于 10 个证书 与存储空间有关
多文件	典型值: 大于 64 个文件 与存储空间有关
多会话密钥	最大支持 8 个会话密钥
证书类型支持	RSA 证书 (1024/2048) SM2 证书
国密算法支持	SM1, SM2, SM3, SM4, SSF33 支持 SM2 协商会话密钥

2.7 指纹与 PIN 管理模式

指纹与 PIN 码的管理，在设备初始化时创建，可设置管理密码，用户密码，指纹最大重试次数,指纹验证级别。

下表列举出管理员 PIN、管理员指纹、用户 PIN、用户指纹之前的权限关系：

权限	功能	操作项	
		管理员指纹	用户指纹
管理员 PIN	创建	√	√
	删除	√	√
	解锁	√	√
管理员指纹	创建	√	√
	删除	√	√
	解锁	√	√
用户 PIN	创建		√
	删除		√
	解锁		√

2.7.1 管理员 PIN 与管理员指纹

管理员 PIN 与管理员指纹拥有设备管理的最高权限。

首次使用 mToken K9 请先验证管理员 PIN 后才能录入管理员指纹，正确录入管理员指

纹成功，下次使用 mToken K9 验证管理员权限时可以选择使用“管理员 PIN”或“管理员指纹”验证。

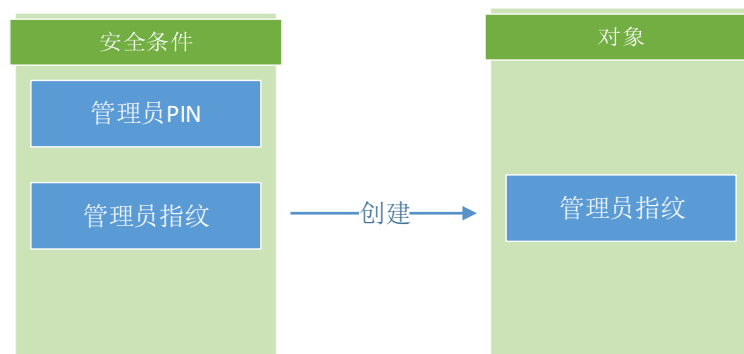
管理员 PIN 与管理员指纹，拥有创建，删除，解锁管理员指纹与用户指纹的权限。

2.7.2 用户指纹

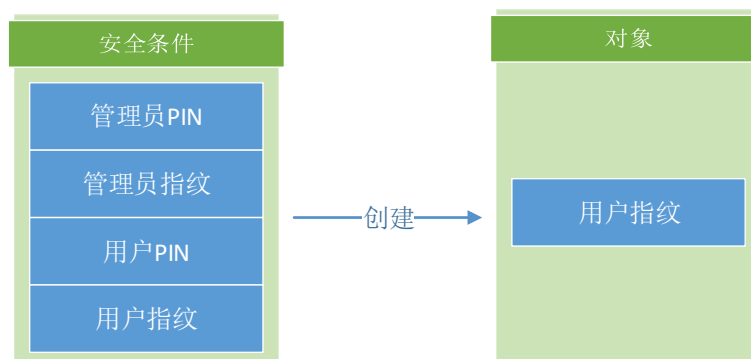
用户指纹在通过管理员 PIN/管理员指纹或用户 PIN/用户指纹验证成功后可录入用户指纹，用户指纹录入成功后，在需要用户权限的验证时，可以使用用户指纹代替用户 PIN。

2.7.3 指纹创建

管理员指纹：

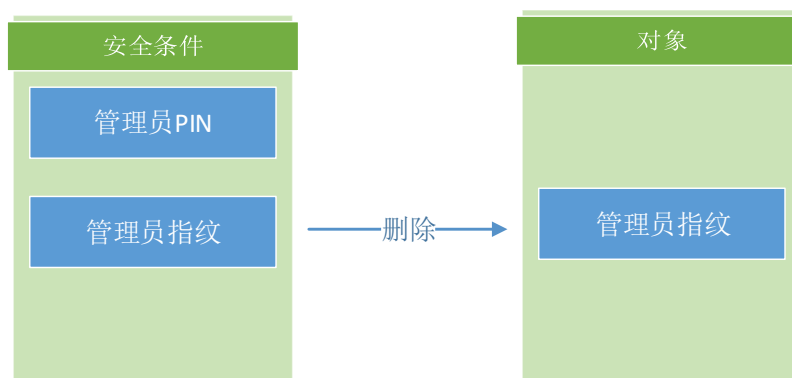


用户指纹：

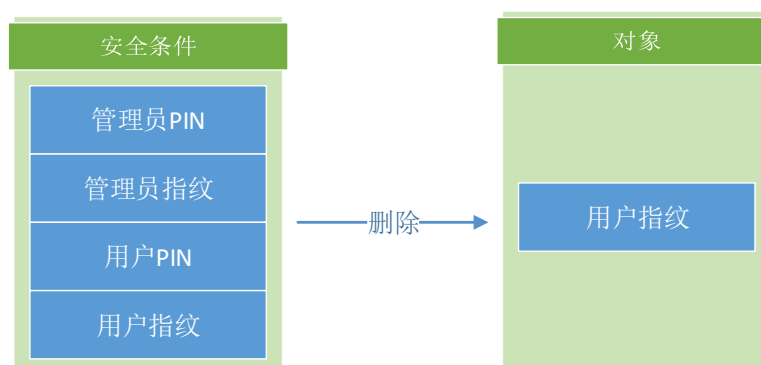


2.7.4 指纹删除

管理员指纹：

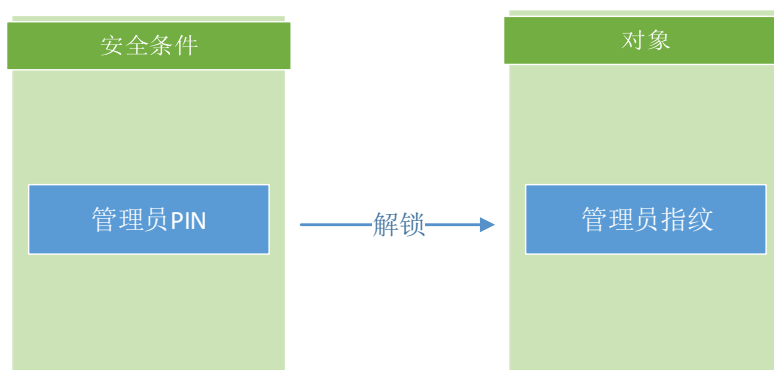


用户指纹：

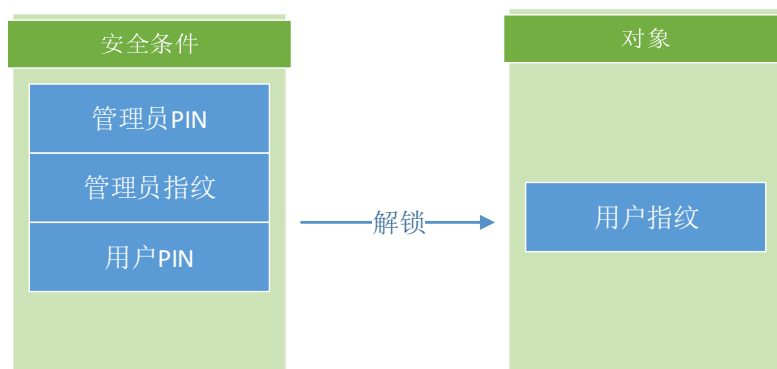


2.7.4 指纹解锁

管理员指纹：



用户指纹:



2.8 中间件支持

- MS CAPI
- PKCS#11 V2.2
- 国密 SKF 接口《GM/T 0016-2012 智能密码钥匙密码应用接口规范》

2.9 典型应用

名称		K9-HID	K9-CCID	K9-CD
通讯协议		HID	CCID	USB Mass Storage
典型应用	电子政务	√	√	√
	电子商务	√	√	√
	邮件加密	√	√	√
	电子签章	√	√	√
	域登录		√	
	VPN 登录		√	

	远程桌面/虚拟桌面		√	
	大数据加密存储应用			√

第三章 产品特点

4.1 指纹 KEY 特点



- 32 位高性能智能卡芯片
- 双因子认证，指纹与硬件；
- 唯一性，指纹代替用户口令，防止非法认证；
- 无需记忆，安全易用；
- 先进的指纹识别算法,识别率高；
- 无驱设备，即插即用；
- 活体指纹鉴别，轻触按压，安全便捷；
- 指纹结合数字证书，数字签名，数据加/解密更安全

4.2 应用特点

mToken K9 提供符合国际标准的应用接口，应用接口适用于 Windows、Linux、Mac OS、国产操作系统等多种操作系统，同时通过“龙脉国密 KEY 证书综合应用插件”接口也适用于 IE 浏览器、腾讯 TT、猎豹、傲游、Netscape、Google Chrome、Apple Safari 等多种浏览器。

4.3 浏览器支持列表

龙脉科技超级插件测试所支持浏览器列表		
序号	浏览器	所有版本
1	 IE 浏览器 IE6, IE7, IE8, IE9, IE10, IE11	√
2	 Mozilla Firefox	√
3	 360 浏览器	兼容模式(IE 内核)
		极速模式
4	 Google Chrome	√
5	 遨游	兼容模式(IE 内核)
		极速模式
6	 猎豹	√
7	 Opera Internet Browser	√
8	 Safari (Windows)	√
9	 Chromium	√
10	 百度浏览器	√
11	 The World	√
12	 QQ 浏览器	√
13	 Airview	√

14	 糖果浏览器	√
15	 CometBrowser	√

第四章 指纹 KEY 与普通 USBKEY 对比

对比项目	mToken K9	(普通型 USB Key)
安全性	通过采集活体指纹验证，避免通过键盘输入密码，防止密码被盗用；	通过键盘输入密码，密码容易被盗取，从而 key 容易被劫持。
	指纹生物特征唯一，防止被他人盗用；	普通 USB Key 密码可以转让，容易造成被动人情泄密，和主动口误泄密；
	USB Key 通过指纹进行确认身份，指纹具有人体生物特征的唯一标识，可以防止责任不明，人员抵赖的情况发生；	普通 USB Key 密码被他人知晓，且 USB Key 被他人拿到，便能够进行非法认证或者操作，由此无法确定此行为是由 key 持有者造成还是被其他不法分子所为；
	指纹特征存储在智能卡芯片中，仅支持指纹验证；	用户密码易被恶意穷举破解；
便捷性	指纹 USB Key 通过指纹进行认证，指纹无需记忆或额外携带，不会遗失；	普通 USB KEY 需要密码输入，密码容易遗忘，且需要通过键盘输入，对密码的复杂度有要求。
	多个指纹认证支持	密码口令通过键盘输入。

第五章 联系我们

公司总部

地址：北京市海淀区王庄路甲1号工控办公楼三层

电话：010-62323636

传真：010-62313636

热线：400-666-0811 (7x24免费热线)

邮箱：longmai@longmai.com.cn

网站：<http://www.longmai.com.cn>

邮编：100083

杭州办事处

地址：浙江省杭州市西湖区文三西路499号西溪风尚5幢420

电话：0571-86908895

邮箱：hangzhou@longmai.com.cn

邮编：310012

广州办事处

地址：广东省广州市天河区黄埔大道中路262号恒安大厦恒福轩14D

电话：020-85272610

邮箱：guangzhou@longmai.com.cn

邮编：510630

成都龙脉

地址：四川省成都市高新区大源国际中心B2栋0706室

电话：028-83225970

邮箱：chengdu@longmai.com.cn

邮编：610000

申请试用

如果您对产品感兴趣，可先申请试用，请到龙脉官方网站填写试用单或直接打电话与我们联系：

试用：<http://www.longmai.com.cn>

邮箱：sales@longmai.com.cn

电话：010-62323636

购买产品

如果您希望咨询产品价格或正式购买产品，可以通过如下方式与销售人员进行联系：

电话：010-62323636

邮箱：sales@longmai.com.cn

技术支持

我们提供了多种方式的技术支持服务，您可通过如下方式向技术人员咨询：

电话：010-62323636-637

邮箱：support@longmai.com.cn