

mToken K9-V

(指静脉 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	4
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	7
2.7 指静脉与 PIN 管理模式	8
2.7.1 管理员 PIN 与管理员指静脉	9
2.7.2 用户指静脉	10
2.7.3 指静脉创建	10
2.7.4 指静脉删除	11

2.7.5 指静脉解锁.....	11
2.7.6 指静脉与证书绑定	12
2.8 中间件支持.....	12
2.9 典型应用.....	13
第三章 产品特点	13
4.1 指静脉 KEY 特点	13
4.2 应用特点.....	14
4.3 浏览器支持列表.....	14
第四章 指静脉 KEY 与普通 USBKEY 对比	16
第五章 联系我们	17
联系方式.....	17
申请试用.....	17
购买产品.....	18
技术支持.....	18

第一章 背景概述

1.1 项目背景

随着互联网技术的不断发展，网上应用日益增多，信息化渗透到工作生活的各个方面，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》规定：“我国各级计算机信息系统须有用户身份鉴别功能，并且三级以上系统需要有两种以上更加严格的身份鉴别机制，如采用人体生物特征（指纹、指静脉）等特殊信息来进行身份鉴别”。鉴于各行业更高标准的信息安全需求，龙脉科技创新研发了指静脉型智能密码钥匙 mToken K9-V。mToken K9-V 将传统的 USBKEY 身份认证功能与指静脉鉴别技术相结合，利用指静脉代替传统密码，可有效避免用户在使用 USBKEY 时，设备遗失、密码泄露和指纹复制带来的安全隐患。同时，mToken K9-V 可实现灵活的应用管理，智能的证书与指静脉绑定，1 对多或多对 1 的指静脉管理，打破了传统的先选证书再认证的模式，有效解决了项目集成中公用 KEY 身份认证的难题，更方便的在项目中集成和使用，真正实现了——KEY 多人使用且安全有效鉴别身份的目的。

为了方便您对本产品的熟练操作和使用，我们建议您仔细阅读以下内容，若需要帮助，请拨打我公司的描述技术服务电话 400-666-0811，我们愿竭诚为您服务！

1.2 产品定位

根据客户需求，mToken K9-V 产品采用具有国密型号的 32 位安全芯片，并结合指




静脉采集器，将指静脉特征技术与数字证书认证相结合，进而实现更高安全标准的身份认证功能。mToken K9-V 使用方法和应用场景与传统 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，是一款集指静脉识别算法、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		
	正面	侧面	铭牌
K 9			

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

硬件参数		
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	≤130mA	
待机电流	≤27mA	
工作温度	-20℃~60℃	
工作湿度	20%~80%RH	
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 位高性能国密安全芯片	
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	
指静脉特性参数		
项目	参数	
指静脉采集方式	开放式采集	
指静脉芯片寿命	1 , 000 , 000 次以上	
指静脉识别方式	1 : N	
拒真率	<0.01%	
认假率	<0.0001%	
识别速度	<1 秒	
处理速度	40 帧/秒	
录入次数	3 次	
存储指静脉个数	管理员指静脉	10 个指静脉特征
	用户指静脉	10 个指静脉特征

2.2.2 产品特性

mToken K9-V 指静脉 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-V 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
- COS 参数

特性	参数
应用	支持多个应用
容器	支持 64 个容器
证书	典型值: 大于 10 个证书 与存储空间有关
文件	典型值: 大于 64 个文件 与存储空间有关
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
指静脉	管理指静脉 10 个 用户指静脉 10 个

2.7 指静脉与 PIN 管理模式

指静脉与 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，指静脉最大重试次数，指静脉验证级别。

下表列举出管理员 PIN、管理员指静脉、用户 PIN、用户指静脉之间的权限关系：

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

2.7.1 管理员 PIN 与管理员指静脉

管理员 PIN 与管理员指静脉拥有设备管理的最高权限。

首次使用 mToken K9-V 请先验证管理员 PIN，然后才能录入管理员指静脉。正确录入管理员指静脉后，下次使用 mToken K9-V 验证管理员权限时可以选择使用“管理员 PIN”或“管理员指静脉”验证。

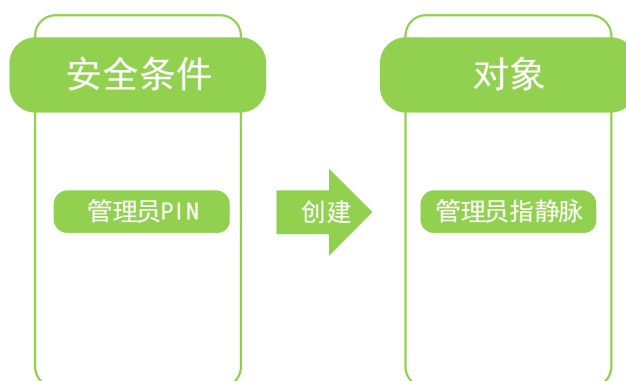
管理员 PIN 与管理员指静脉，拥有创建、删除、解锁管理员指静脉与用户指静脉的权限。

2.7.2 用户指静脉

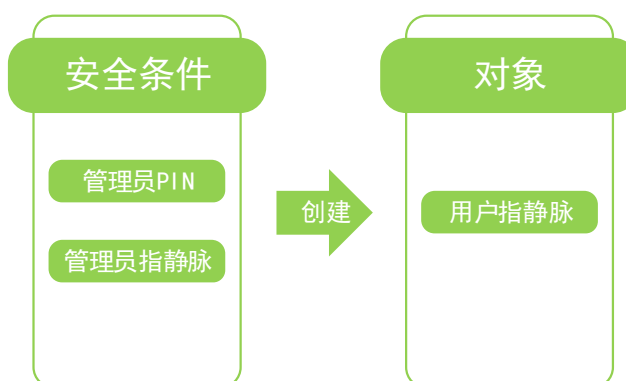
用户指静脉在通过管理员 PIN/管理员指静脉或用户 PIN/用户指静脉验证成功后可录入用户指静脉，用户指静脉录入成功后，在需要用户权限的验证时，可以使用用户指静脉代替用户 PIN。

2.7.3 指静脉创建

管理员指静脉：

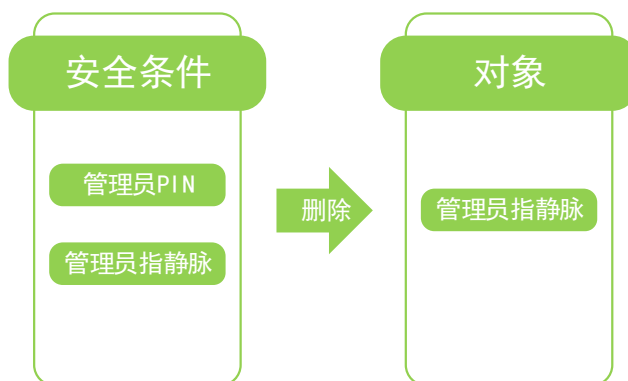


用户指静脉：

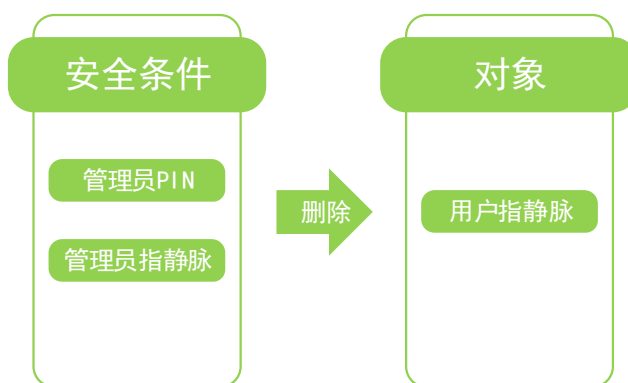


2.7.4 指静脉删除

管理员指静脉：

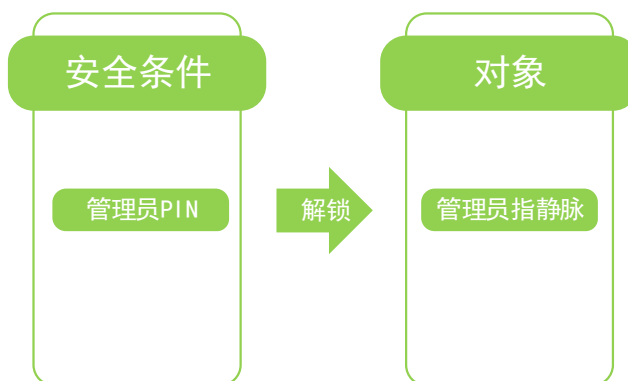


用户指静脉：

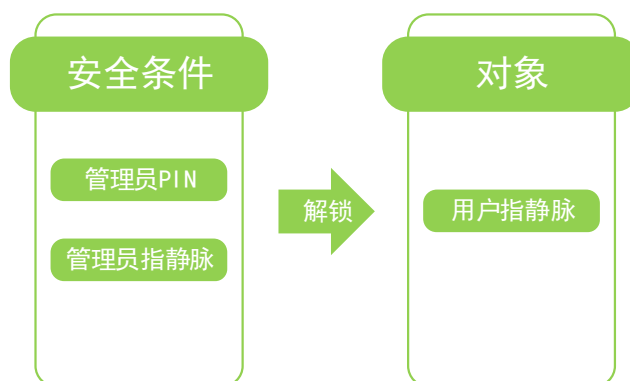


2.7.5 指静脉解锁

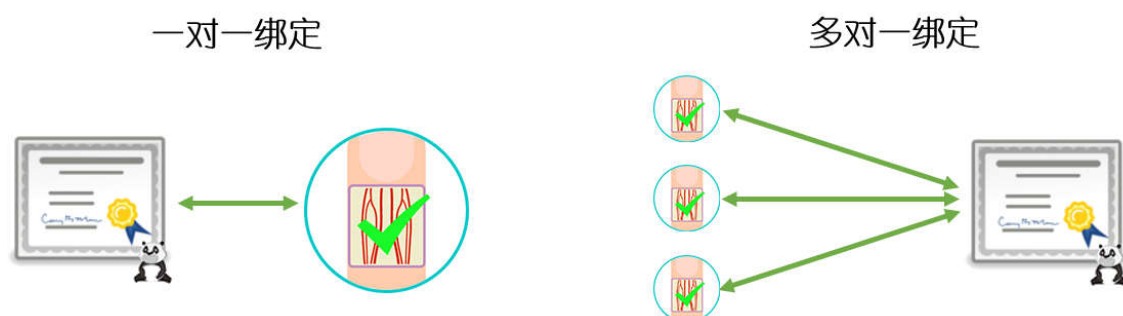
管理员指静脉：



用户指静脉:



2.7.6 指静脉与证书绑定



注：一张证书绑定一个指静脉，同时支持一张证书被多个指静脉绑定，但一个指静脉不能绑定多张证书

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-V-HID	K9-V -CCID	K9-V -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 指静脉 KEY 特点

- 32 位高性能安全芯片
- 基于人体指静脉生物特征认证；
- 唯一性，指静脉代替用户口令，防止非法认证；
- 无需记忆，安全易用；
- 先进的指静脉识别算法，识别率高；

- 无驱设备，即插即用；
- 活体指静脉鉴别，安全便捷；
- 指静脉结合数字证书，数字签名，数据加/解密更安全
- 不易受手指状况影响，如干湿手指、手指蜕皮等；
- 非易获取生物特征鉴别，更加安全可靠。

4.2 应用特点

mToken K9-V 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	 傲游	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 指静脉 KEY 与普通 USBKEY 对比

对比项目	mToken K9-V	指纹型 USBKey	(普通型 USB Key)
安全性	<ul style="list-style-type: none"> ● 采集和验证活体指静脉，避免了键盘输入密码的过程，更好的防止密码被盗用。 ● 指静脉生物特征唯一，防止被他人盗用； ● USB Key 通过指静脉进行确认身份，指静脉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； ● 指静脉特征存储在安全芯片中，不允许读出； ● 非接触式，不存在复制风险。 	<ul style="list-style-type: none"> ● 通过人体指纹模板进行 ● 指纹作为生物特征，破解难度较大，且不容易被盗用； ● 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； ● 指纹特征存储在安全芯片中，不允许读出； ● 接触式，有被复制的风险。 	<ul style="list-style-type: none"> ● 通过键盘输入密码，密码容易被盗取，key 容易被劫持； ● 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； ● 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； ● 用户密码易被恶意记录或者劫持。
便捷性	<ul style="list-style-type: none"> ● 指静脉 USB Key 通过指静脉进行认证，指静脉属于人体特征，无需记忆或额外携带，不会遗失。 ● 支持多个指静脉认证； ● 人群适用性强，精度更高，不受手指表面情况影响，如 	<ul style="list-style-type: none"> ● 指纹 USBkey 通过指纹进行认证，指纹属于人体特征，无需记忆或者额外携带； ● 支持多个指纹认证； ● 受手指表面情况影响，如蜕皮、干湿手指等。 ● 指纹特征作为表 	<ul style="list-style-type: none"> ● 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。 ● 密码口令通过键盘输入。

	蜕皮、干湿手指等。 <ul style="list-style-type: none">● 非体表特征,不易获取。	面特征,易被获取。	
--	---	-----------	--

第五章 联系我们

联系方式

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

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