mToken CPK Card Technical Paper

Century Longmai Technology Co., Ltd.

Revision Record

Date	Revision Version	Sec No.	Change Description	Author
2015/02/15	V1.0		Initial Version	Longmai ITD

Contents

mToken CPK Card

Overview

Today, the authentication market is seeking for portable device with increased efficiency and a broad range of on-board security applications like digital signature, user identification, secure on-line transactions and physical access control application.

As one of the leading digital security providers Century Longmai now offers all the power of a multi-application contactless card and smart card USB PKI token in a single device; developed based on current & expected market trends and consumer requirements. These hybrid mToken CPK card support for two different 2FA technologies: Digital Certificates (smartcard chip-based PKI) and contactless MIFARE - delivering a robust solution in form of a secure smart card USB token and MIFARE card for applications such as: micropayments, access management, Network security, and automatic fare collection systems in public transport; individual identification and physical access control in corporate, banking and government facilities.

Thanks to the full support for middleware, all mToken CPK card model support the PKCS#11 cryptographic standard on the Linux, Mac OS and Windows environments, users benefit from unparalleled level of integration with multi-platform based applications with a smartcard chip, it performs well in multiple working environments, such as online payment, identity authentication and information management.

It is a secure innovative real deal for those who require an effective combination of security and portability in protecting important personal, financial and company information.

Product Introduction

Century Longmai's mToken CPK Contactless card allows faster and more convenient transactions by eliminating the need for contact between the card and the scanner/reader. The demand and acceptance for this type of card is rapidly growing, with major deployments in applications such as micro-payment, physical and logical access control, government and corporate IDs, and automatic fare collection (AFC) - majorly designed

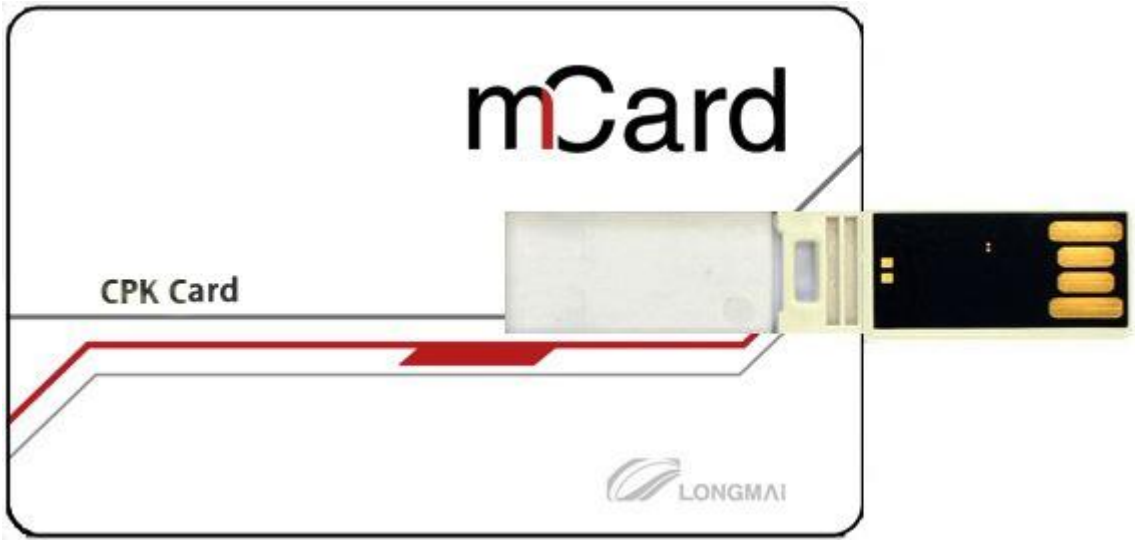
for two applications, i.e. PKI identity authentication and as a contactless utility card; users could make authentication and management based on One-Card to do jobs like documents signing, access control, micro-payment, and etc.

mToken CPK card has been developed with a peculiar emphasis on user convenience, fast transaction speed, exceptional reliability for frequent usage, security against fraud and cost effectiveness. It combines the functions of smart card USB token and the features of contactless card.

It is one of today's powerful devices to be used for digital certificate management, private information protection, and physical & virtual access control.

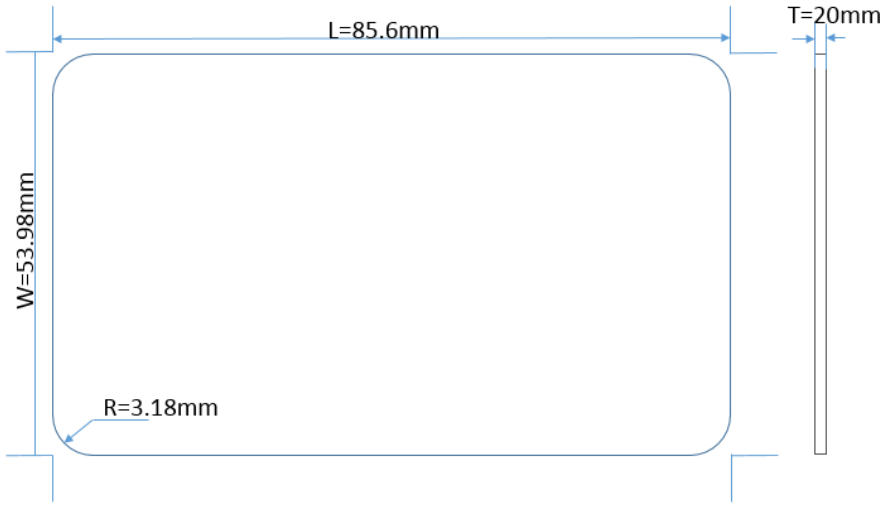
With adopting the technology of integrated packaging, mCard CPK Card is proved waterproof, dustproof and quake proof.

Product appearance



mToken CPK Card Size

- L：85.6mm（85.47mm-85.72mm）
- W：53.98mm (53.92mm-54.03mm)
- T： 20mm (± 0.03mm)*
- R： 3.18mm (± 0.30mm)



** implies the card's parameter is customizable based on user's requirements*

mToken CPK Card Models

Century Longmai offers customization service to all customers and partners on mToken CPK Card. The following are our existing models:

	mToken CPK-ID	**mToken CPK-M1**	**mToken CPK-CPU**
Contactless chip model	Identification Card Read-only identity card	Mifare 1 Contactless logic encryption card	CPU Contactless smartcard

Product Advantages

	Traditional USBKEY	**Smart Card**	**CPK Card**
Support for PKI Application	YES	YES (but requires a card reader)	YES
Multi-application	NO	YES	YES
Certificate application speed	Fast	Slow	Fast (same as USB KEY)

Contactless application speed	--	Fast	Fast (same as Smartcard)
Cost	Low	High	Low

Contact USB Key

Support for multiple Operating system environments including:

- Windows
- Linux
- Mac OSX

COS Features

- Self-developed Intellectual COS
- Compliance with ISO 7816-4 communication protocol.
- Support for different Cryptographic algorithms DES, 3DES, AES128/192/256, SHA1/SHA256/SHA384/SHA512, RSA(1024/2048)
- Support for multiple applications, multiple containers and multiple certificates.
- Support for encryption, decryption, signature, authentication, key exchange, key wrapping.
- Support for X.509 v3 certificate & PKCS12 data format.

Supporting middleware

- Microsoft CAPI
- PKCS#11 support for multiple systems.

Contactless Chip

Features

- Operating Frequency: 13.56MHZ
- Communication speed: 106KB Baud Rate

- Anti-collision Mechanism, support for multiple cards' operation at the same time.
- Read & Write operating range: 2.5-10cm
- ISO/IEC14443 1/2/3/4 standards
- Meet ISO/IEC14443Anti-collisionMechanism

M1 Features

- 16 sections, each section is divided into 4 parts, each part could store 16 bytes.
- Each section has its own password and access control
- Each card has its own 32-bit Serial number
- Anti-collision, multiple cards' simultaneous operation supported
- No battery needed, build-in antenna, logic encryption and communication logic circuit
- Support for multi-applications
- Number of reads Unlimited
- Number of writes is 100 000
- Data retention for 10 years

CPU features

- Owns unique CPU processor and chip OS
- Multi-application card, each application is separate multi-level dictionary can be built
- Supporting multiple file formats, such as binary file, fixed length record file, variable length record file, circular file
- Support for PBOC 3.0, EMV standards for e-wallet, debit and credit applications.
- Number of reads Unlimited
- Number of writes is 100 000
- Data retention for 10 years

Technical Specification

Overview

mToken CPK (defined as Contactless PKI Card) is a lightweight contactless smart card with USB token that provides a both contactless and strong authentication PKI based solutions. It is the most secure and portable cryptographic contactless device in the market.

The mToken CPK enables digital signatures, email encryption, micropayments, and other PKI applications. The Flappable USB Token acts as a point of convergence for public key certificates and associated keys with built-in Smart Card chip all cryptographic operations, such as RSA (up to 4096bits), SHA-1, SHA-256, AES-128/192/256 and 3DES, are performed in the hardware rather than in the PC or terminal. This ensures that all sensitive credentials protected by cryptographic keys cannot be hacked or sniffed - allowing ultimate security to be achieved.

Features

- Cryptographic contactless card and USB token
  - Embedded smartcard chip
  - User memory: 64KB
  - ISO 7816 Compliant
  - Supports commands for cryptographic operations, authentication, and access control
  - Supports Mutual Authentication with Session Key Generation
  - Cryptographic algorithm support including: 3DES (ECB, CBC); MAC; SHA-1, SHA-256; AES-128, 192, 256; RSA-512, 1024, 2048, 3072 and 4096 bits
  - On-board RSA processor that supports fast key generation, signature and encryption
  - Provides ease of integration with MULTIPLE applications such as Internet Explorer, Mozilla, Microsoft Office, etc
  - Customizable PIN code
- Host Interface
  - PS/SC Compliant (Plug and Play)
  - USB 2.0 Full Speed

  - Smart card power supply through USB port
- Token form factor
  - Extremely light weight: 6 grams
  - Pocket size: 53.5 mm x 15.7 mm x 7.8 mm
  - Keychain hole
  - Tamper-evident casing

The following list provides a summary of the technical information about mToken CPK

Category	Parameters
Contact smartcard chip Parameters	
Power Supply	USB Power Supply
Working Voltage	5V USB port power supply
Working Current	80-150mA
Operating Temperature Range	0 - 70°C
Storing Temperature	-20 - 85 °C
Casing Material	PVC
Communication Protocol	USB
Interface Type	USB 2.0 / 3.0
Processor	32-bit smartcard chip
Certificate storage Capacity	192K
*External Storage Capacity	CD：2M-8M, Default 2M USB Flash memory: 4G-32G
Contactless chip Parameters	
Power Supply	Build-in Coil Power Supply
Operating frequency	13.56MHZ
Operating range (Read & write)	2.5-10cm
Working Temp range	0 - 70 °C
Storage Temp range	-20 - 85 °C
Casing	PVC
Communication Protocol	ISO 14443 Type A protocol
Processor	Read-Only; Logical encryption or CPU chip

Storage Capacity	M1： 1K or 4K CPU： 4K or 8K
Data retention	10 years

General application of mToken CPK

mCard CPK's main functions are divided into two parts, the first part is two-factor authentication PKI function, and the second part is Mifare card functions.

Smartcard chip PKI-based functions:

- Identity authentication
- Digital signature/Seal
- Data encryption/Decryption
- Email encryption/Decryption
- Other PKI solution functions
- Contactles MIFARE functions:
- Entrance control
- Internal restaurant charge
- Internal Parking lot charge

Other Mifare card solutions

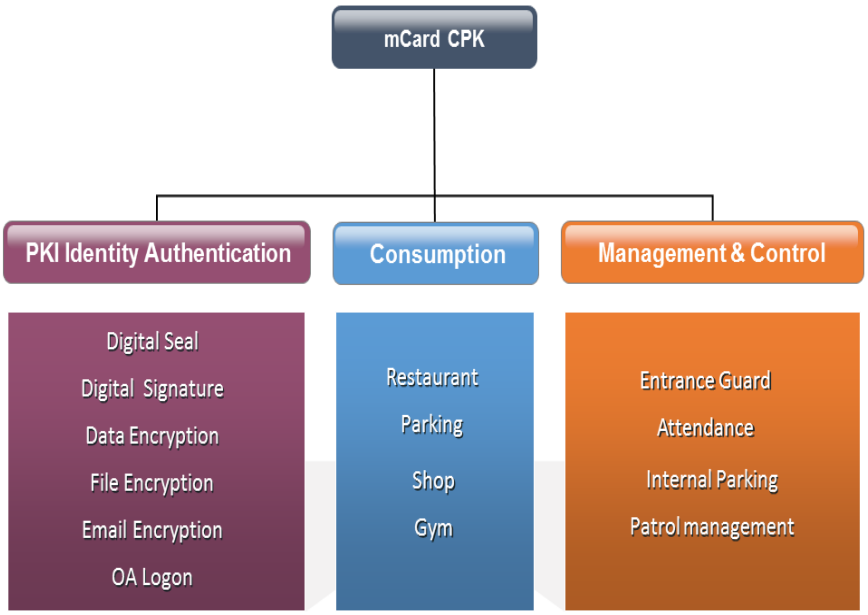


Fig 0-1 mToken CPK Contactless card Applications

mCard CPK Solution Features

- All in One card solution
- High security level 32-bit smartcard chip
- High performance
- Waterproof; dustproof and quakeproof
- Convenient, users do not need to take many cards
- Cost effective
- Prevent Unauthorized Access

Product General Features and Benefits

mToken CPK cards are compatible with contactless standard technology, Public key infrastructure, allows for smooth integration of new multi-application services used in different markets.

For Government institutions or private enterprises committed to take their IT Security and access control infrastructure to the next level with robust multiple form factor

solutions, mToken CPK is the straightforward solution to combine Logical Access Control management and Physical Access Control management in a single Contactless card with USB Cryptographic Token device.

User access is granted in various system levels such as application level, documents, databases, etc.

- Encryption of access codes and passwords
- Creation of a table of physical persons that can have access to the system as well as creation of the authentication process.
- Definition of the single and only one access code for the system use (single sign-on)
- Control system of data integrity
- Support of digital signatures and PKI infrastructure
- Data encryption over unsafe networks
    - Unparalleled Integration with Identity and Access Ecosystem:
    - Support for Certificate Based two factor authentication
    - Compliance with industry standards
    - Support for Windows, Linux & Mac Operating Systems
    - Cost-effective Innovative MIFARE implementation
    - Strong Smart card Security
    - Smart Card integration with PKI application services such as Email, Web, VPN, etc.
    - Reliability and Stability – mToken CPK Card adopts reliable and stable hardware, software and advanced technology to gurantee application security.
    - Standardability – mToken CPK Card is developed based on international standard.
    - Scalability, seamless migration to newer infrastructure.
    - Provide employees with this contactless PKI-capable smart card to verify their identity and control access to sensitive data. With extensive integration capabilities and PKI authentication support, the mToken CPK product delivers unparalleled authentication control to government and private entities.

Key Features

Unique Card Identification Number & PIN

Support for standard card readers.

Operating distance: Up to 100mm or 4 inches (Distance varies depending on the reader and chip/card antenna geometry)

Anti-cloning: Unique serial number for each card to ensure the uniqueness of each device.

High data integrity during communication and data transmission

Data retention of 10 years with write endurance of 100,000 cycles

True anti-collision (An intelligent anti-collision algorithm allows operation with multiple cards exposed to a single antenna field simultaneously

Extreme Encryption

This solution provides ultimate security with AES 256 encryption, the USB key is based is smartcard chip hardware encryption module.

Broad system and Hardware Compatibility

mToken CPK is one of our industry-leading identity products delivering a compatible solution with all operating systems & RFID scanners/ Readers

High-Quality, Flexible Design

This solution is portable, maintains an ISO9000 quality certification, and offers flexible connections via USB or contactless MIFARE.

Provide employees with this contactless PKI-capable smart card to verify their identity and control access to sensitive data. With extensive integration capabilities and PKI authentication support, the mToken CPK product delivers unparalleled authentication control to government and private entities.

mToken CPK Supporting Solutions

This Information is available through our registered partners, please contact us.

About Century Longmai

Established in 2003, Century Longmai Technology Co., Ltd is one of the most leading information security device vendors in China with over 12 years experience developing latest generation of digital security solutions and products for secure information access and transmission. Our product portfolios include PKI dongles, wireless PKI tokens, OTP tokens, smart card, smart card readers, electronic document protection solution, software license dongles, Smartcard readers and OEM services. Proved to be secure and convenient, our solutions and products are dedicated to help customers build safe, efficient and sustainable networks, financial systems and enjoy secure access to data and information everywhere whenever they want.

Century Longmai Technology Co., Ltd

3rd Floor, GongKong Building, No.1, WangZhuang Road, Haidian District, Beijing, China
Postcode: 100083
Tel: (86) 10-62323636 | Fax: (86) 10-62313636
Sales E-mail: info@longmai.net Support E-mail: support@longmai.net
Website: http://lm-infosec.com