

**FEITIAN**

**Feitian Smart Card**  
*Product Brochure*





# OUR TEAM

**PROFESSIONAL  
SMART TEAM**



CHIP TECHNOLOGY ANALYSIS

SMARTCARD BUSINESS ANALYSIS

EMV PROJECT

JAVA PROJECT

DOT NET PROJECT

CRYPTOGRAPHY AND ENCRYPTION

STRONG AUTHENTICATION

MIDDLEWARE FOR SMARTCARD API

SMARTCARD READERS

SMARTCARD RELATED DEVICES

**FEITIAN**

# OUR PRODUCTS

**SIM CARD** *for GSM*

**RUIM CARD** *for CDMA*

**JAVA CARD**

**.NET CARD**

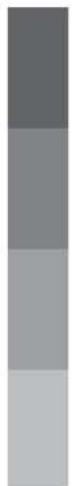
**PKI CARD**

**CREATIVE CARD**

**PAYMENT CARD**

**ID CARD**

**RELIABLE FEITIAN  
SMART CARDS**



over 600 million Chinese

# GSM SIM CARD



## SIM & RUIM

A Subscriber Identity Module (SIM) is part of a removable smart card, also known as SIM Cards, for mobile, telephony devices and mobile phones. SIM cards securely store the service-subscriber key (IMSI) used to identify a subscriber. The SIM card allows users to change phones by simply removing the SIM card from one mobile phone and inserting it into another mobile phone or broadband telephony device.

The use of SIM cards is mandatory in GSM devices. The equivalent of a SIM in UMTS is called the Universal Integrated Circuit Card (UICC), which runs a USIM application, whereas the Removable User Identity Module (RUIM) is more popular in CDMA-based devices.



It is well-known that the primary function defined for SIM card is holding the identity of the subscriber and authenticating the mobile station with respect to the network. Besides, the SIM also be used in quite a number of applications, such as allowing program execution to be protected against manipulation, making it possible to store data including phone numbers, short message and personal configuration settings for mobile telephone, and acting as the carrier for secure supplementary services used within mobile telecommunications.

As the average selling prices of earlier generations of SIM cards decline due to the effects of intense competition, we had been continuously looking to develop and market new generations of microprocessor cards with greater capabilities and attractive price to mobile communication operators all over the world.

## SIM CARD FEATURES

- COMP 128 -1/2/3 and other relevant authentication algorithm
- GSM Phase 2+ and SIM Toolkit(STK) for SIM application development
- Anti-clone mechanism to be safeguard against fraud
- Subscriber identification, phone number and SMS saving, voice and data, and other basic services
- Dynamic STK menu download and several value-added applications

## SIM CARD STANDARDS

- ISO7816 1/2/3
- GSM 11.11 - Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface
- GSM 11.12 - Specification of the 3 Volt Subscriber Identity Module – Mobile Equipment (SIM – ME) interface
- GSM 11.14 - Specification of the SIM Application Toolkit for the Subscriber Identity Module –Mobile Equipment (SIM – ME) interface
- GSM 11.17 - Subscriber Identity Module (SIM) conformance test specification
- GSM 03.48 - Specification of security mechanisms for the SIM application toolkit, Stage 2

1

**FEITIAN**

mobile phone subscribers make phone calls with

# CDMA RUIM CARD

Asian operators have led the world in the adoption of RUIMs. China Unicom was the first CDMA operator using the RUIM. A RUIM card would make CDMA more attractive to consumers and would also open the door to better roaming contracts between CDMA and GSM networks, allowing the best possible global coverage for all cellular customers.

The RUIM card provides flexibility to switch phones by simply removing the RUIM card and slipping it into another card-enabled phone. The new phone would then be able to make and receive calls on the user's account without having to go through the carrier for activation. With the appropriate roaming agreement in place, a user could have several phones and switch from a CDMA phone to a GSM one by inserting the dual-mode RUIM card, thus making it available for user to borrow a friend's phone but call with his RUIM card, or even switch to another carrier and keep his or her old phone. The new carrier would simply issue the customer a new RUIM card to use in his or her existing phone. The only requirements are that the phone is unlocked and compatible with the frequency band of the new carrier. People enjoyed the convenience associated with the simplified access.

The benefit of having an RUIM for both GSM and CDMA is that the subscriber can have one phone book, one number, as well as the same interfaces and menus. No matter what technology the subscriber is using, convenience and ease-of-use are crucial to customer satisfaction and to avoid churn.

Smart cards represent security for business and mobile users alike. CDMA subscriber can easily pay their bills with their mobile phones if the CDMA operator guarantees security for their personal data and creates the right partnership with the smart card provider and the bank.

While the subscriber can change handsets at will, the RUIM remains the only element in the network that is completely controlled by the operator.



## RUIM CARD FEATURES

- Support CAVE algorithm
- Support OTA (Over-the-Air) and SMS PRL update
- Support dynamic UTK menu download and value-added services based on UTK
- Support EVDO

## RUIM CARD STANDARDS

- ISO7816 1/2/3
- GSM 11.11
- GSM 11.14
- GSM 11.17
- IS-683-A
- IS-820/Addendum
- TIA/EIA/IS-95-A/B
- ANSI-41
- 3GPP2 C.S0023
- 3GPP2 C.S0015



2

# JAVA CARD



With the development of open-platform operating systems for smart cards, which contain an application programming interface and an interpreter for execute applets, it allows software programmers to create applications based on a standard protocol that can run on any smart card, irrespective of the card manufacturer.

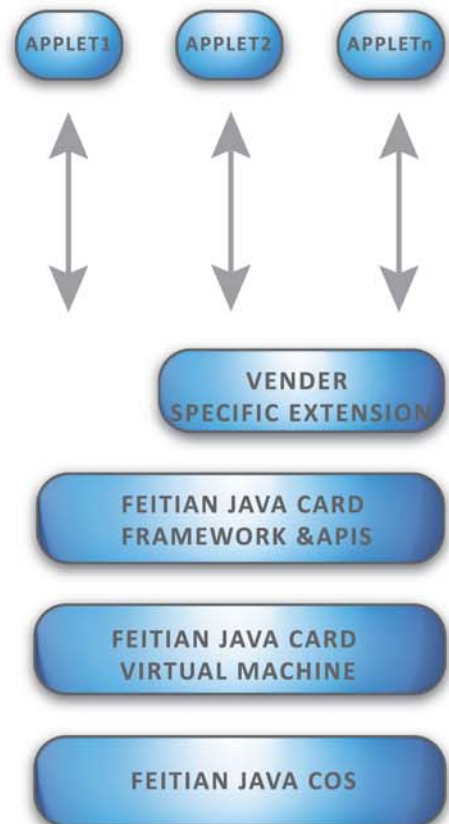
It was common realized that using the Java programming language the development of smart card applications is simplified and improved. Feitian Java Card is referred to as a platform, not an operating system, which supports a set of specifications for a subset of Java technology, for example Java Card Virtual Machine Specification, Java Card Runtime Environment Specification, as well as the Java Card API Specification, and allows multiple applications from same or different vendors to securely coexist.

## JAVA CARD FEATURES

- FTSmart /CO1, SmartMX Platform, Java Card™ 2.2.1
- GlobalPlatform 2.1.1
- DES, 3DES, and RSA 2048 bits,
- On-board Key Generator
- FIPS 140-2 compliant RNG
- Supports both standard ISO 7816-3 protocols T=0 and T=1, as well as PPS negotiation corresponding to transmission speeds from 9600 to 115,200 bauds
- Contactless interface type A, T=CL communication speed 106, 212, and 424 kbps
- T=CL protocol supports automatic waiting time extension management and random UID generation
- Mifare Emulation 1K with proprietary API to access to Mifare memory

## TYPICAL APPLICATIONS

- Credit/Debit Payment: CFCA certified EMV compatible payment application Java Card applets.
- Strong Authentication: PKI Enabled Java Card applets for Strong Authentication applications.
- Electronic ID: With Built-in contactless interface, Feitian Java Cards can be implemented into Electronic Identification systems easily.



we serve with what you are familiar with

# .NET CARD

**F**eitian .NET Card brings the functionality of the .NET platform into smart card. It is natively supported in Windows Vista and works as a seamless companion to the Microsoft .NET environment and service-oriented architectures. It runs a streamlined version of the .NET Framework to provide customizable two-factor authentication, full cryptographic capabilities and support for both on-card applications and off-card services seamlessly within the Windows environment.

Now with the Feitian .NET Card, there is no need to know details about the smart card and card reader, or know about low-level APDU communications, organizations can easily secure their networks from end to end while dramatically reducing development time, implementation costs and complexity.

The .NET Card technology provides a secure platform to connect the various participants in some new markets like, and offers the security and control that will be vital for the commercial implementation of next generation entertainment services. Feitian .Net platform has multi-language functionality to allow cross functionality between applications and services developed in any language supported by the .NET framework, including Visual Basic .NET, C++, C#, JavaScript and J#, thus providing flexibility and usability to great extents.

The Feitian .NET Card platform will allow developers to build quick, easy and secure links between different types of multimedia devices and applications, for example, digital rights management for online games, music and video-clips, as well as the roaming applications such as multimedia messaging combined sound, pictures and small video sequences, email downloads etc.

With the advanced technology infrastructure, Feitian .NET Card acted as the server layer and designed to enable a range of applications to be automatically downloaded and installed onto the smart card.

The .NET Card development is an important element of the Feitian vision for a new dimension of smart card applications, and reinforces the Feitian commitment to open platform technologies.

## .NET CARD FEATURES

- Fully development with Microsoft Visual Studio to offer seamless integration for on-card application and management
- Compliant with ECMA-335 libraries and state-of-art smart card operating system
- Allow multiple programming languages within Microsoft .NET Framework
- Support event, task, application lifetime, garbage collection and application process domain control
- Provide complex data structure as collection, stack, hash etc.
- High Speed Smart Card chip built in
- User-defined Security Access Control Policy and APDU command
- On-card encryption algorithms including AES / DES / 3DES / SHA1 / SHA256 / MD5 / HMAC / RSA 2048
- Support single/double precision floating point operation functions



## PKI CARD



The PKI, also known as Public Key Infrastructure, is adopted widely in strong authentication applications. Due to sensitive data, such as private keys, are very important to the PKI system, high security smart cards are normally selected as the *carrier* to perform the role.

Feitian's PKI card is specially designed for PKI-based applications, as it is obvious that the combination of smart card technology with public key infrastructure does provide a greater and stronger level of protection against hackers than a standalone public key system. All sensitive credentials and private keys are stored inside the smart card chip and cannot be accessed from outside, thus reaching the ultimate security for both intranet, extranet, and Internet applications, including secure access, authentication and data transmission through encryption technology as well as physical access and other extensive used applications.

### PKI CARD FEATURES

- Support ISO 7816 compliant cryptographic operations, authentication and access control
- Support ISO 7816 part 12 contacts USB electrical interface
- Support cryptographic algorithm of DES, 3DES, MD5, SHA-1, SHA-256, RSA 1024, RSA 2048
- Support secure messaging ensured confidentiality between the smart card and the application
- Support standard PKCS#11 and MS CAPI interface, ease of integration for compliant software
- Support cryptographic service provider for Microsoft smart card enrollment for Windows smart card user and smart card logon.

### TYPICAL APPLICATIONS

PKI technology enables secure access, communications and transactions over internal or open networks using digital certificates to identify users and keys or algorithms to encrypt information transmitted over the network. Some of the information stored in the Feitian PKI Card is in the form of a number composed of "ones-and-zeros" referred to as the "private key", which is part of a two-key system used to encode and decode sensitive information. The security of such systems is relied on the safeguard of the private key. Typically, after the card-holder authenticates the PKI Card by supplying a PIN number, the private key will then be used to encrypt any sort of transaction using the card.

Cards using PKI technology are offered to customers requiring the highest level of security, such as public authorities and corporations implement online network access services, wireless network operators and financial institutions implementing e-commerce systems, and are capable of enabling new types of secure transactions using digital signatures. Feitian PKI Cards have obtained the highest levels of certification relating to analysis of the card's ability to handle attacks and prevent covert channels

# Create Your Own Algorithm For Your Card

## CREATIVE CARD

An algorithm is informally defined as a computer program that calculates something. A set of pre-defined algorithms, such as RSA, DES, Triple-DES, etc., are normally provided by smart card chip OS providers for data encryption purpose. Apart from data encryption itself, smart card users may need more algorithms other than those bonding with the chip, to get more flexibility matching their various requirements. Feitian Creative Card is a special platform that helping those users who want to be CREATIVE in building their own algorithms into the chip.

Feitian Creative Card platform comes with mass-user-memory chips, comparing with those traditional 16K/32K or 64K smart cards, Creative Card offers more space for users to create their own algorithm that can be located inside the smart card chip and accessible same as those pre-defined common algorithms.



### FEATURES

- ISO/IEC 7816 CPU Card
- 120K SuperFlash non-volatile Memory
- FIPS 140-2 Compliant RNG
- High Speed Data Communication
- Faster time to market
- Flexible memory architecture
- Greater security
- Voltage Regulator and Detectors
- Frequency, Brown-out, Temperature, UV Light, and Glitch Detectors



# PAYMENT CARD



Credit or debit payment cards bring us lots of convenience, comparing with traditional bank notes. But both card holders and issuers have to face the fact of frauds in the payment card industry. Hopefully, more and more key players from the payment card industry are inclined to secure card transactions by upgrading traditional mag-stripe card to smart card.

In view of the card upgrading implementation, cost and complexity of the smart card application development are the top two difficulties. Since the day that smart card came to the industry, the low-level assembly language is the most common platform for developers, which limit the resources and the slow down the progress.

Being an innovator in the smart card industry, Feitian keeps searching after to have the two problems solved with better solutions, lower down the

cost of the card and its development by adopting latest smart card technoligis, such as Java and .Net. As a result, more and more high level programming language developers are able to touch the smart card development without have difficulties while "talking" to the chip.

Meanwhile, Feitian keeps working closely with the payment industry leaders, the chip providers and card issuer banks, and it makes Feitian growing up quickly to become a qualified payment card expert to deal with major payment card projects, based on various payment smart card specifications.

## FEATURES

- ISO/IEC 7816
- ISO/IEC14443
- EMV or other Payment Specificaitons
- Credit and/or Debit Applications
- e-Purse Applications
- Contactless Payment (optional)
- Mass on-chip Secure Memory
- Multi-Application Mechanism
- Multi-Level Access Control
- Card-Terminal Cross Authentication Mechanism
- Affordable for Mass Implementation and Customization



A Technology Serving 1 Billion ID Holders

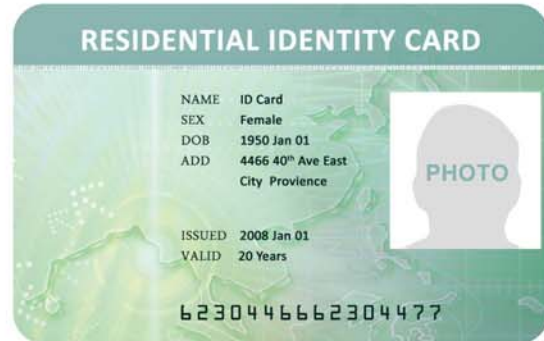
# ELECTRONIC ID CARD

Identity document, also called a piece of identification (ID), is a document used to verify aspects of a person's identity. There are many kind of ID cards in our social life, such as National ID, citizenship card, driving license, or even a passport is another kind of internationally recognized ID.

Being a kind of important identity document, all ID issuance authorities are seeking new technology to improve its security, to avoid illegal duplication and frauds. As a result, smart card technology and products are becoming the first choice in the industry.

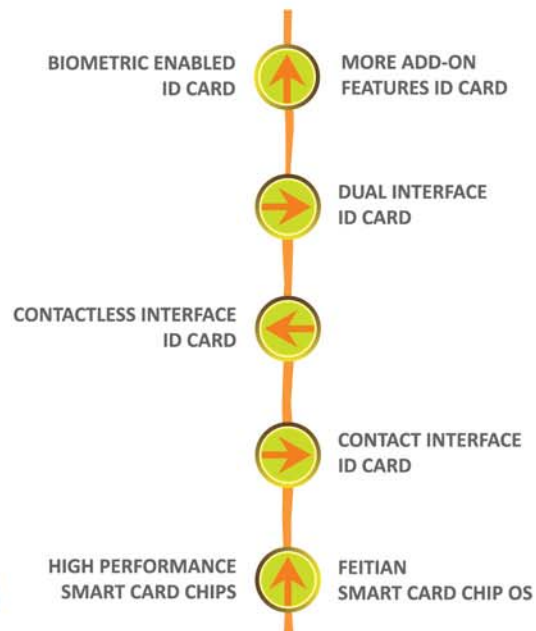
By partnering with one of the biggest National ID technology provider in China, Feitian developed a series of on-chip applications to meet various of ID Card requirements, applicable for the usages from employee ID to electronic passport.

Electronic ID projects usually target a huge amount of acceptants, thus the cost becomes sensitive. Feitian is specialize in providing qualified products and solutions according to customer's budget. We offer not only the the card itself but also customization development of on-chip applications (COS).



## FEATURES

- ISO/IEC 7816
- ISO/IEC14443
- CC EAL5+ Smartcard Chip Available
- Low Power/Low Voltage Design
- High Reliable EEPROM for Data Storage
- High Speed Data Communication
- RSA DES 3DES AES Algorithms
- Mass on-chip Secure Memory
- Multi-Application Mechanism
- Multi-Level Access Control
- Card-Terminal Cross Authentication Mechanism
- Affordable for Mass Implementation
- Biometric Application (optional)
- USB 2.0 Interface (optional)



8

## About Feitian

Established in 1998, Feitian is dedicated of being the leading innovator of smart card and chip operating system based security technologies and applications. Combined with the latest technologies Feitian has designed and developed its DotNET Card and Java Card with best-of-breed applications, implementing into fields ranging from card payment, strong authentication, telecommunication, electronic identification and more.

Feitian cooperates closely with global leading smart card chip providers, serves valuable customers with the world's latest technologies via it expanding sales and services network internationally.

Feitian Technologies Co., Ltd  
[www.FTsafe.com](http://www.FTsafe.com)