Rechargeable Fingerprint Authenticated Card

(MyGoldWallet Card) Specification

londoncoin.io

Document History

Document Name: MyGoldWallet Card Specification

No	Version.	Date	Contents	Location	Reason	By
1		2018.09.19	Spec. Draft Release			
2						
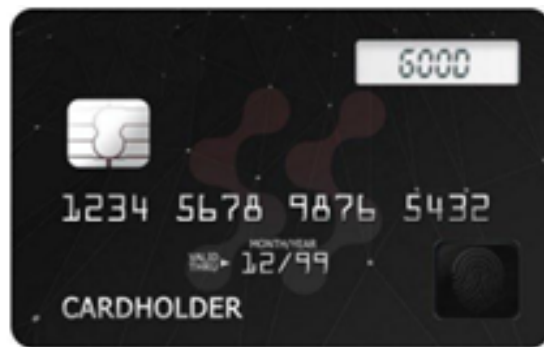
Table of Content

MyGoldWallet Card Specification

1. Summary

□ MyGoldWallet Card (Hereafter called as "MGW Card") is a Smartcard which recognizes user's fingerprint with a built-in rechargeable battery. If previously registered fingerprint matches the users' fingerprint, the MGW Card functions fully. Otherwise, the MGW Card works with limited functions.

□ MGW Card is equipped with a re-chargeable battery without requiring additional power source to operate.

□ MGW Card has an LCD display. Users can find out if the fingerprint matches easily as well as can see the fingerprint registration process in detail.

□ Nowadays, the credit card can be a risk to be lost or stolen, but fingerprint authentication card with biometric authentication allows to use only the registered user. Therefore, it significantly reduces the risk to be lost or stolen for a card owner.

□ Also, the fingerprint authentication is done with the MGW Card directly, thereby minimizing the fingerprint information to be compromised.

2. Characteristics and Specification

- With biometric authentication MGW Card, it enhances the security of the smartcard use
- Reducing the risks of card to be lost or stolen
- Operating the card by comparing the user's fingerprint with registered one
- If the fingerprint does not match the pre-registered one, the card will work with limited functions.
- High performance fingerprint authentication sensor
  - 8.37mm X 9.19mm size fingerprint sensor
  - 160 X 160 pixels, 508 DPI
- High reliability fingerprint authentication algorithm
  - 1/50,000 FAR
  - 3% FRR
- The form factor is same as a regular credit card, even with battery and fingerprint authentication.
- Sensor
  - Thickness: 0.84mm (Regular credit card size)
- MGW Card maintains its authentication status for only 15 seconds after the fingerprint authentication is proved normally, and after then, it limits security features.
- Displaying the status of the fingerprint match on the screen
- Maximum 5 fingerprints can be registered
- Specification for the smartcard support
  - ISO/IEC 7810
  - ISO/IEC 7816
  - ISO/IEC 14443
  - Class A, B Support
- MGW Card functions normally for 30 days with a single battery charge, provided that MGW Card is used 30 times per a day.
- MGW Card also meet EuroPay, Visa, Master (EVM) card's physical requirements

3. **Major Functions**

- Pushing a power button to operate the card

- If MGW Card recognizes the fingerprint and matches the fingerprint to display it on screen by showing that the smartcard is functioning normally.

- MGW Card has several loaded applications. Only fingerprint authentication related applications will work with the fingerprint authentication, and other applications which do not require the fingerprint authentication will work without the fingerprint authentication.

- 2 level authentication process, consisting of 1st level (fingerprint authentication process) and 2nd level (user identity by a smartcard)

- Possible for fingerprint registration and re-registration

- Works with an internally built-in rechargeable battery

- Providing a USB port charger

- MGW Card satisfies all the physical requirements of a smartcard (thickness, tension, torsion, etc.) as well as anti-fire protection from the battery.

4. Applications

MGW Card can be used in the following areas.

- Cold storage wallet for cryptocurrencies
- ID/Password replacement for trading crypto currencies in an exchange site and for an application such as Metamask
- Entrance card, Employee card, Student card, etc. for personal identification
- Transportation card, public auction card, etc. for a public service sector
- Benefit card for the disabled, voucher card, health care card, etc. for a health and welfare sector
- Pre-paid card, direct payment card, credit card, and online settlement card, etc. for a financial sector

5. Card Structure

A fingerprint authentication card system consists of a fingerprint authentication card and a battery charger.

5.1 Fingerprint Authenticated Card
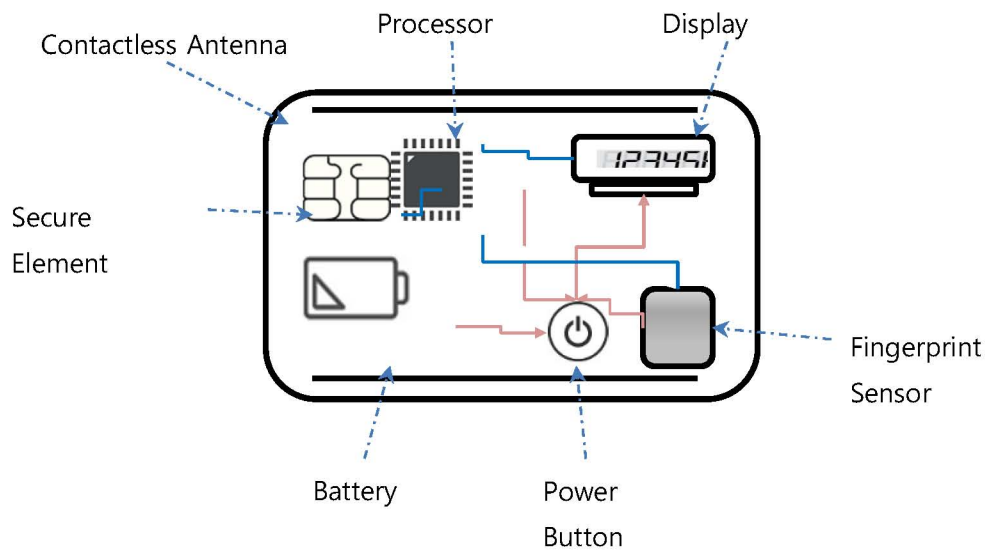
- Secure Element: Enables financial transaction, personal identification etc.
- Fingerprint Sensor: Attaching and detecting user's fingerprint
- Display: Displays Success/Fail results about fingerprint authentication
- Fingerprint Processor: Generates fingerprint template and compare/authenticates
- Contactless Antenna: Secure Element Contactless supports
- Power Button: Turning on and off for the MGW Card
- Battery: Secondary rechargeable battery for the MGW Card
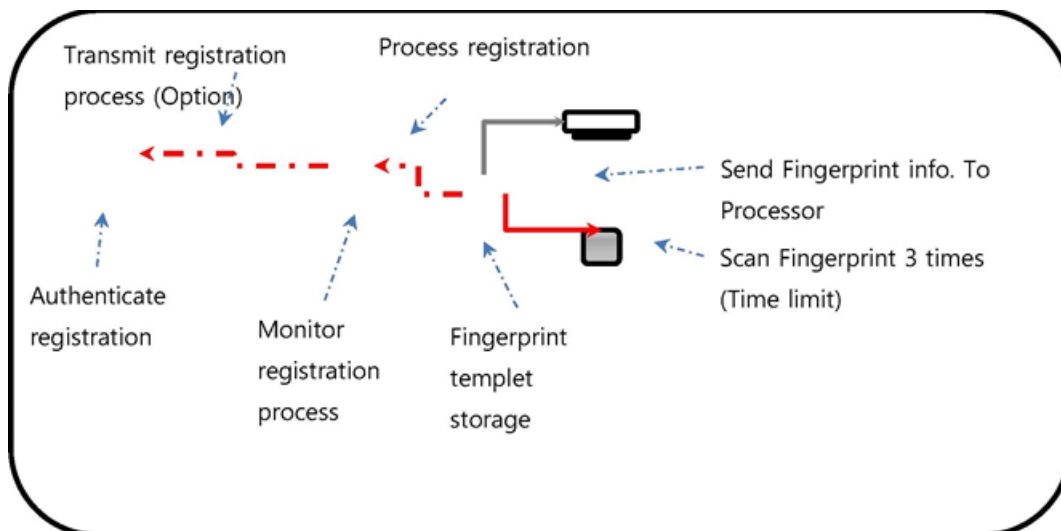
5.2 Battery Charger

- Battery Charger is designed to use a USB type dongle which has the connector to battery with an LED, where it turns on green when charging is complete, and red during the charging process.

6. Card Process

6.1 Fingerprint registration

(1) Configuration

- **[Function]:** Registering user's fingerprint to an MGW Card. The MGW Card can be operated normally only once the fingerprint is registered.
- **[Operation Process]:** Firstly, turn on the power button by pushing, and place the fingerprint on the sensor 3 times. Once the fingerprint is registered, then power will be turned off automatically.
- **[Time Limit]:** Fingerprint input needs to be done within 5 seconds. If there is no input for 5 seconds, the MGW Card will be immediately turned off.
- **[Display]:** the number of fingerprint scanning will be displayed every time when scanning is done.
- **[Fingerprint Storage]:** Fingerprint information is cryptically stored in a Secure Zone.
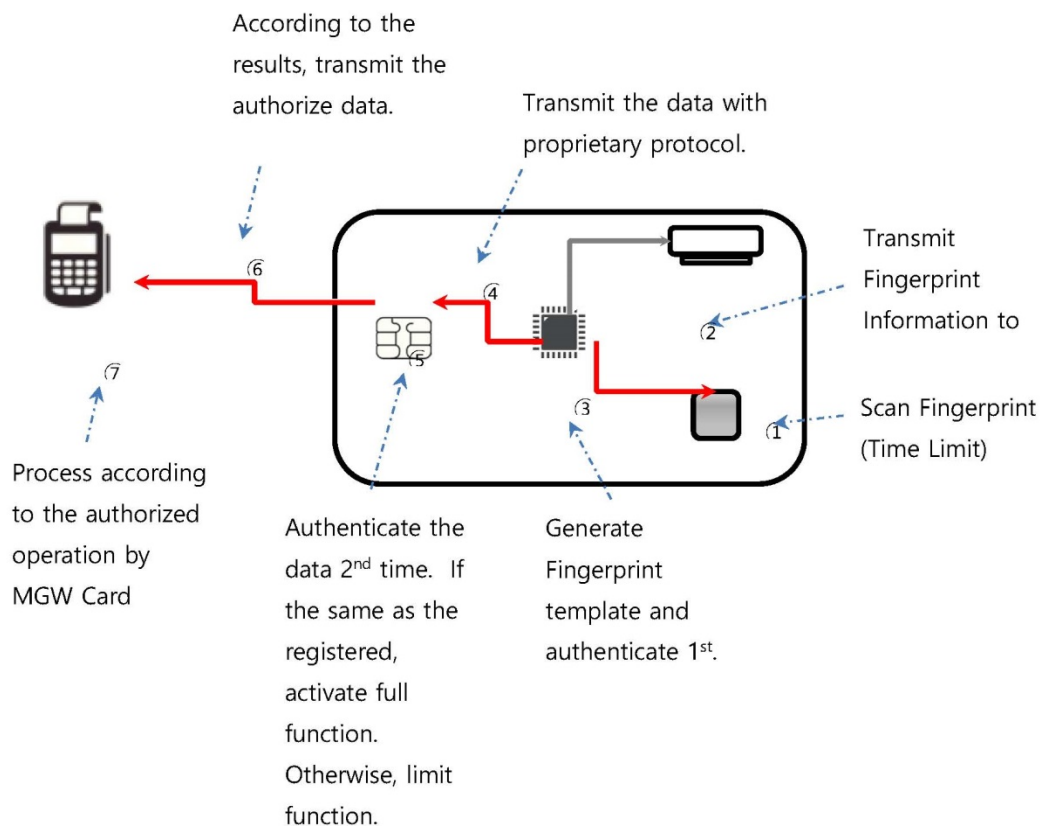
(2) How to use

Sequence of Card Operation	Display	User Operation
	888888	-Register Fingerprint. -Turn on Power. -Button Scan 3 times with the same fingerprint
	No-Id	
	Id 1-1	
	Id 1-2	
	Id 1-3	
	888888	

6.2 **Fingerprint Authentication**

- **[Function]:** Process which compares and authenticates the registered fingerprint with an input fingerprint

- **[Operation Process]:** Firstly, turn on the power button by pushing, scan the fingerprint. Once the result is displayed, insert it to the card terminal. Payment, password, ID etc. will be processed with a terminal and an MGW Card.

- **[Fingerprint Authentication]:** If an input fingerprint matches a registered one, the MGW Card can be used normally. Otherwise, the MGW Card can be used with limited functions. For example, the MGW Card can be recognized without payment and ID detection.

- **[Time Limit]:** Fingerprint input needs to be done within 15 seconds. The MGW Card will be turned off after the authentication is done.

According to the results, transmit the authorize data.

Transmit the data with proprietary protocol.

Transmit Fingerprint Information to

Scan Fingerprint (Time Limit)

Process according to the authorized operation by MGW Card

Authenticate the data 2nd time. If the same as the registered, activate full function. Otherwise, limit function.

Generate Fingerprint template and authenticate 1st.

(2) How to use
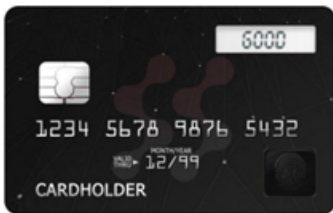
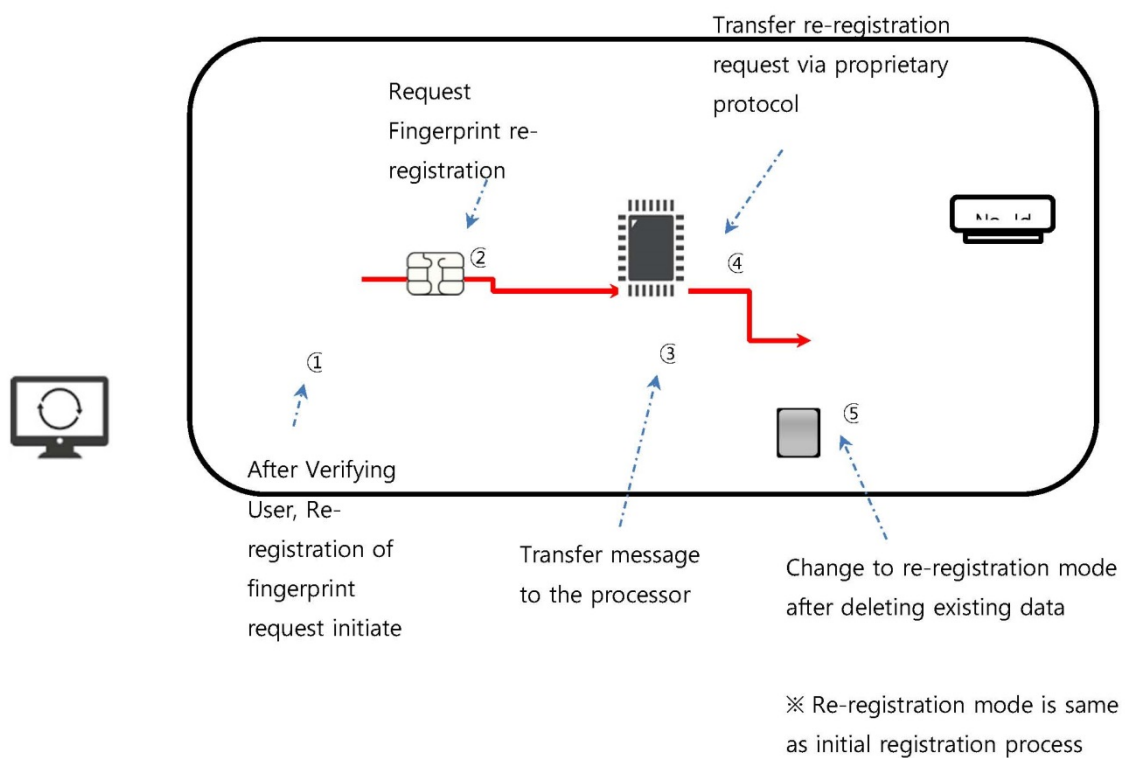| Sequence of Card Operation	Display	User Operation
	888888	Pressing power button
	Auth	Registering fingerprint
	Good FAIL	Authenticating Fingerprint
	Good	Touching Card terminal to use
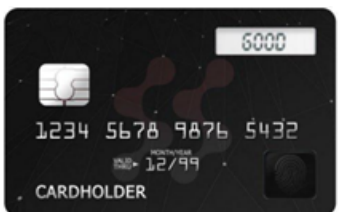
6.3 **Fingerprint Re-Registration**

(1) Sequence of **Fingerprint Re-Registration**

- **[Function]:** Deleting current data to re-register the fingerprint in an MGW Card
- **[Operation Process]:** Firstly, Turn the power on by pushing the power button, and re-register the card to the terminal. Once existing data is deleted, the power will be turned off automatically. Turn the power on again to proceed with the fingerprint registration process.
- **[Time Limit]:** Register the MGW Card within 5 seconds to the terminal. Otherwise, MGW Card will be turned off.

(2) How to use

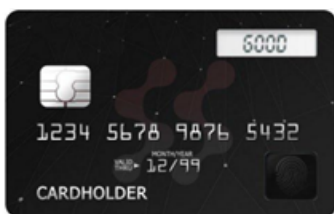| Sequence of Card Operation	Display	User operation
	`Auth`	Pushing Power button and touching it to the terminal
	`888888`	Pushing power button again
	`No-Id`	Registering fingerprint by scanning the same finger 3 times
	`Id 1-1`	
	`Id 1-2`	
	`Id 1-3`	
	`888888`	MGW Card turns off automatically

7. Smart Card

The MGW Card has an internal smart IC Chip which enables security function as well as various applications. The hardware and software structure are shown in the below.

```
┌─────────┐ ┌─────────┐ ┌─────────┐ ┌─────────┐ ┌─────────┐
│ Traffic │ │   ID    │ │ Royality│ │ Banking │ │   ...   │
└─────────┘ └─────────┘ └─────────┘ └─────────┘ └─────────┘
┌─────────────────────┐ ┌──────────────────┐ ┌──────────────┐
│                     │ │   Java Card API   │ │    GP API    │
│  Operating System   │ ├──────────────────────────────────┤
│                     │ │    Java Card Virtual Machine      │
└─────────────────────┘ └──────────────────────────────────┘
┌────────────────────────────────────────────────────────────┐
│            Microprocessor + security module                 │
└────────────────────────────────────────────────────────────┘
```
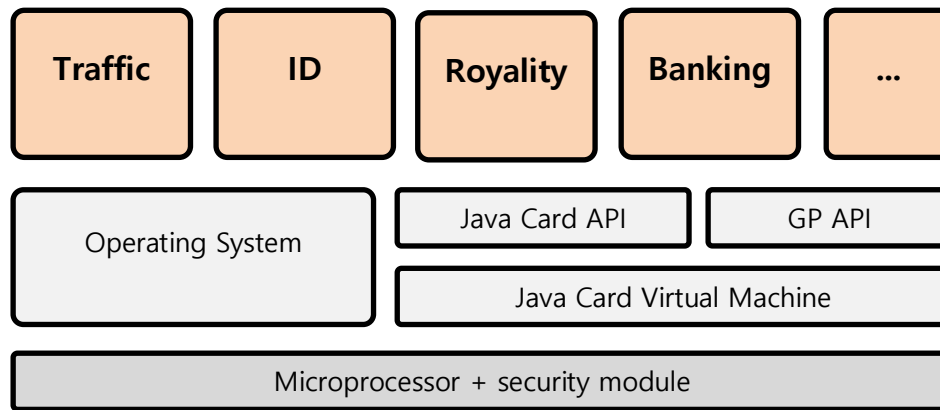
- Smart IC Chip consists of a microprocessor and a security module as well as software OS for a smart card that enables data storage and processing capabilities.

- Smart IC provides 4 security mechanism.
    1) Confidentiality: Prohibits information leak or do not release it to unauthorized personnel
    2) Authentication: Authenticate whether a sender or a receiver is authorized or not
    3) Integrity: Guarantees that the data received is not tampered with from the sender
    4) Non-repudiation: Protects the senders claim that the information is not sent when the receiver received correct information

- Unlike a card without OS, a Java Card OS based smart card enables to run various application via applet, applicable to traffic, ID, entrance control, and banking.

- MGW Card has 4 security mechanisms and Java Card OS is loaded into the smart card chip. Therefore, traffic, banking, ID, and other various value-added services can be loaded on the card.

Appendix

1. Card Type

(1) MS (Magnetic Stripe) Card

- On the back of the card, a magnetic strip (MS) is attached, in which it saves small amount of data except fatal problem is existing in terms of security since it is easily copied.
- Magnetic strip width is 12.5mm, and one magnetic strip consists of three tracks where each track and the purpose of use is defined by ISO7811 specification.

(2) IC (Integrated Circuit) Card

- An IC card is equipped with IC Chips, enabling to use large data and applets compared with an MS Card. ISO7816 specifies the number of terminals where the total number of terminals are 8, but in real usage 6 terminals are used.
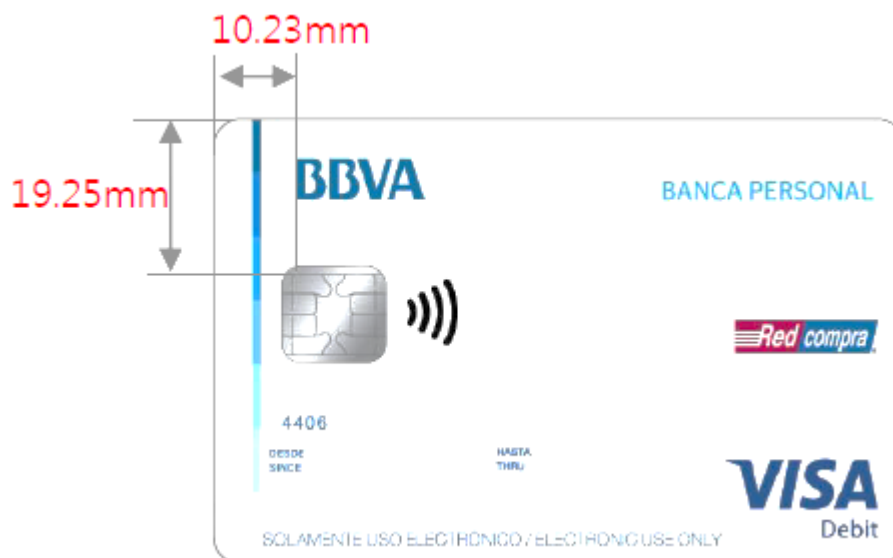
2. Card Specification

- All the cards are manufactured with ISO7810/10373 specification

- ISO7810: Physical requirements of Card body

- ISO10373: Physical testing

(1) Requirement

Item	ISO standard
Width	85.47 ~ 85.72
Height	53,92 ~ 54.03
Thickness (MS Card / IC Card)	0.68 ~ 0.84
Corner Bar	2.88 ~ 3.48
Border (Burr)	0.08 within

(2) Reliability Test (Card Physical Characteristics)

- [Peel strength (N/cm) measurement]**:** When the overlay is separated from the card body by a width of 10 mm and peeled at a line speed of 30 cm/min, it should be 3.5 N/cm or more.

- [Measurement of Bending and Torsion]: It must be repeatedly applied with a constant force (bending, torsion) 1,000 times from the edge of the card, so that there is no functional or apparent abnormality.
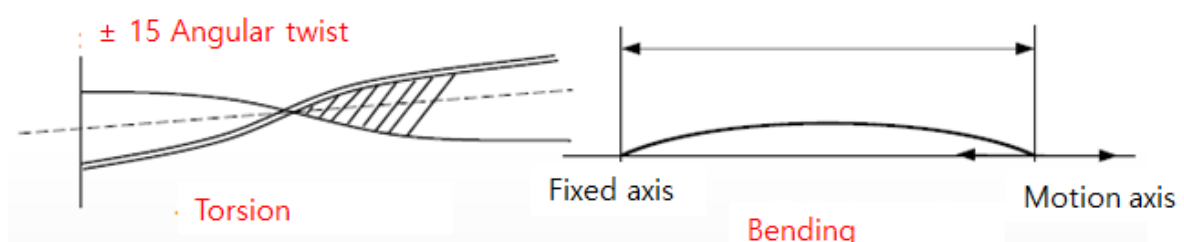
- [Measurement of thermal stability (low temperature and high temperature)]: To measure the durability of the card, it should be stored at high temperature (55 °C) and low temperature (-35 °C).

3. Chip specification

Item	Detail List
CPU	• SecuCalm-16bit
Co-processor	• Tornado-E
Memory	• Flash : 320KB • RAM : 9KB
CC Certification	• EAL 6+ ASE_TSS.2
CMOS process	• 80nm
Memory reliability	• Read/Write over 500,000 times, Store 25 years
Data transmission speed	• 106~848Kbps
Module Size	• 5.00 ㎜ × 4.80 ㎜
Module Thickness	• 0.25 ㎜±0.01 ㎜
Interfaces	• ISO/IEC 7816 • ISO/IEC 14443 : Type A/B
HW Support Security	• ECC, RSA, DES / 3KEY(TDES), AES
Security	• Ability to defend against external attacks such as abnormal temperature, frequency, and voltage attacks, such as chip reset and subchannel attack • ISO/IEC 14443 and ISO 10373-1