Card Testing INTERNATIONAL
AN ISO/IEC 17025 LABORATORY

Card Testing International Ltd
Level 4, 105 High Street
PO Box 30 356
Lower Hutt 5040, NZ

Phone: *Asia/Pacific* +64 4 903 4990 *North America* (800) 438 9036 **Email:** info@cardtest.com **Website:** www.cardtest.com

Smart Cards

A smart card is any card containing an embedded integrated circuit (IC), often referred to as a chip, or microprocessor. The incorporation of ICs into plastic cards has brought with it several advantages: the first being the ability to store a greater amount of data; and the second being the addition of useful advanced security features. Some new smart cards can contain information on several accounts, as well as instore credits or points systems. Typically smart cards come in two sizes; ISO/IEC ID-1 type cards which are 85.60 mm by 53.98 mm, and ID-000 type cards which are 25 mm by 15 mm, both being 0.76 mm thick. Smart cards fall into two distinct categories: contact cards and contactless cards.

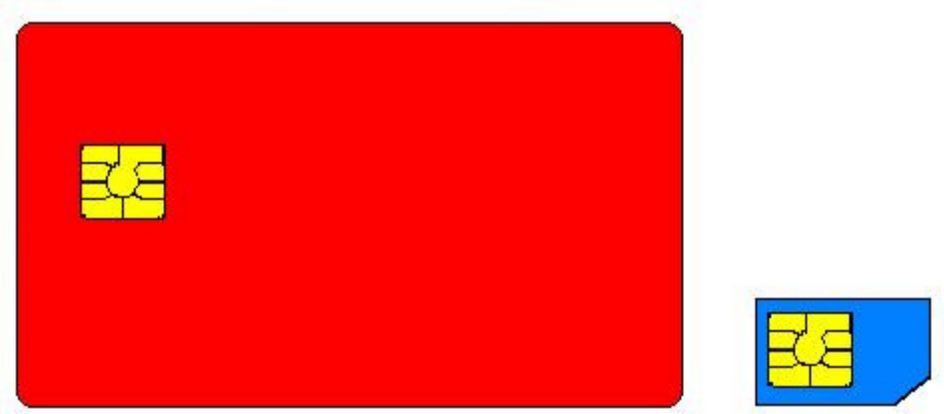

Figure 1. ISO/IEC contact ID-1 style card, left, next to an ID-000 card (not to scale)

Contact Cards

Contact cards have a series of small pads, which provide an electrical connection with a reading device, as can be seen below in figure 2. The use of contact card technology is becoming more prevalent, with a growing number of new credit/debit card companies incorporating it in their products. This technology can also been seen in everyday devices such as cell phone SIM cards. To ensure reliable function on all different types of card readers, a set of ISO/IEC standards have been developed for smart cards. To further improve compatibility between past and present payment systems the payment brands; Europay, MasterCard and Visa created a set of specifications for smart cards called the EMV system. The company EMVco was then setup with the specific purpose of maintaining this system.
EMVco is now owned by American Express, JCB, MasterCard and Visa.

Card Testing INTERNATIONAL
AN ISO/IEC 17025 LABORATORY

Card Testing International Ltd
Level 4, 105 High Street
PO Box 30 356
Lower Hutt 5040, NZ

Phone: *Asia/Pacific* +64 4 903 4990 *North America* (800) 438 9036 **Email:** info@cardtest.com **Website:** www.cardtest.com

The Integrated Circuit

A smart card IC is typically around 1cm², consisting of several contact pads that link to the microprocessor and other additional hardware underneath. Their shape and size are defined by The ISO/IEC 7816 standards, as well as defining what signals can be sent and received to achieve basic functionality. The chip has internal memory (usually EEPROM), allowing the retention of data when in a powered off state. No internal power source exists on the chip, so in order to access the internal data, the reader must provide the required power.

General Chip Layout

VCC – Power Input
GND – Supplied ground
RST – Reset communications pin
VPP – Formerly a programming pin, now used as a Single wire protocol (SWP) pin for telecommunications.
CLK – Clock signal input, for synchronising internal circuitry and data transfer.
I/0 – Data input/output pin.
AUX1/AUX2 – Additional I/O pins.

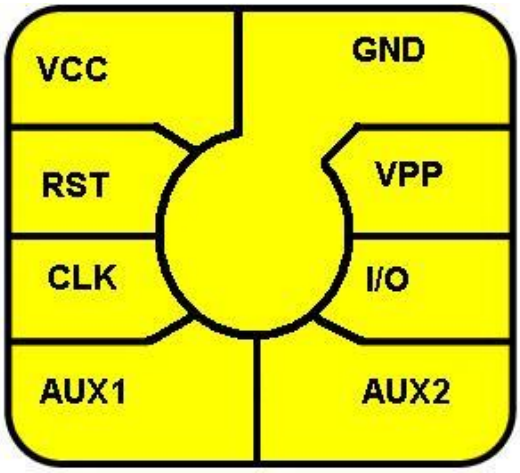

Figure 2. Smart Card Contact diagram

Contactless Cards

Contactless smart cards work in a slightly different manner to contact cards, in that they use radio waves to communicate with a reading device. This allows for the card to be read at a distance (up to 75 mm for type proximity cards, or between 1 and 1.5 meters for vicinity cards), as no physical contact with the reader is actually required. As with contact cards, they contain integrated circuits and have security encryption. These characteristics make them quick and easy to use, which has made them popular in the transport and identification sectors.

Figure 3. Internal view of a contactless smart card, with the antenna connected to the IC module.

Card Testing International Ltd
Level 4, 105 High Street
PO Box 30 356
Lower Hutt 5040, NZ

Phone: *Asia/Pacific* +64 4 903 4990 *North America* (800) 438 9036 **Email:** info@cardtest.com **Website:** www.cardtest.com

Power

Contactless cards do not have an on-board power source, so they must receive their power from an external source. The required power is acquired via resonant inductive coupling, which involves the reader generating a magnetic field, using a coil and an alternating current supply. If a second coil (the smart card) enters this magnetic field, then some of this energy can be utilised to power the internal circuitry.

Security

Although it costs the banks more to produce a smart card than a traditional magnetic stripe card, the additional security offered massively reduces the amount of fraud cases the banks must deal with. This added security comes from the increased storage capacity and processing power of the card. When using a smart card, security measures come into play at all levels of the transaction:

- Firstly the card exchanges encrypted information with the reader, to ensure that both parties involved are legitimate.
- A PIN number is usually entered to provide authentication prior to any major transaction taking place (cards often have a function allowing users to engage in several minor transactions before being prompted to enter a PIN. Also smart cards used in the transport sector do not usually require a PIN, for speed of transaction purposes).
- The transaction being carried out is encrypted, which keeps the process and information being exchanged secret.

This process of certifying that both parties involved are legitimate, as well as ensuring all data transferred is encrypted, makes it hard for man in the middle attacks to be carried out successfully.

With new technology always comes a new method for cracking it, the most important way to ensure data security in the future is for manufacturers to make cards as tamper resistant as possible, and those designing payment systems to continue to incorporate features to counter such attacks.