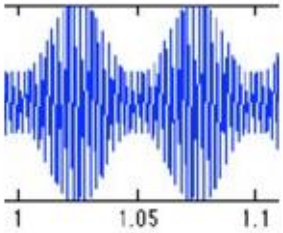
Smart Card Types

By: FT Automation Canada



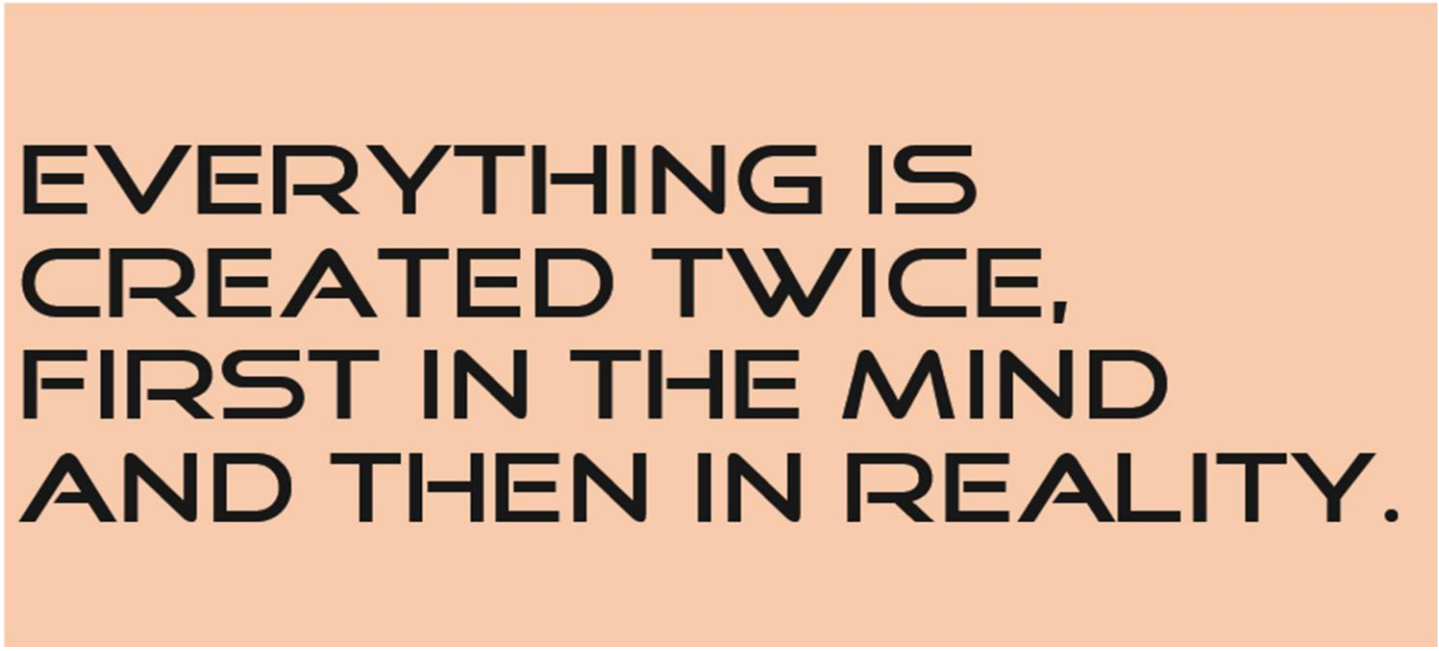
FT Automation engineers have seasoned skills to design, fabricate, integrate and deliver automation systems.

FT Gurus

July 5, 2022

Contents Page

Everything is created twice, first in the mind and then in reality.



1. Card Types

Smart cards are an evolved next generation cards from the old breed of identification cards that were derived from the Physical ISO/IEC standard 7810. This standard specifies the physical properties of identification cards, such as material properties, temperature resistance, and the dimensions of different card formats that are ID-1, ID-2, and ID-3.

We will introduce a variety of cards evolved from the ID-1 format as new forms of Identification Cards have been later developed and combined different features in one single card. The sudden removal of magnetic stripe cards and their reading terminals from the infrastructure is not a great idea, instead the introduction of smart cards with new technology implementation added to the embedded classic magnetic stripe cards can prove to be more pleasant and practical to users since the sudden transition to new technology overnight maybe not be practical. This hybrid breed of cards had combined both the new and classic forms of Identification Cards.

Since new terminals can't read old cards and old terminals can't read new cards, and the fact that many users still use the old cards, new terminals that support both the old cards and new cards have been developed. Old cards were gradually removed from the infrastructure, while new cards are now undergoing mass production.

The transition from old contact smart cards, as per Figure 1, to new contactless smart card should facilitate reliable and practical propagation of both new cards and new card readers. At some point in time only the new readers and new cards should be implemented in the Identification Card Infrastructure. During this transition, all electrical and mechanical specifications are mitigated and accounted for in ways not to interfere with the infrastructure operational quality and performance reliability.

Figure 1 Contact based card and reader.

2. EMBOSSED CARDS

Identification Cards with text embossed on them enable transfer of name and card number into paper by using simple pressing mechanical device, it was the work of old days. Characters spacing and locations are specified under the ISO/IEC 7811 standard. Those standards maybe customised for certain applications. The Embossed Number of the card is located in Zone 1 per the Figure 2 below, where the bottom 4 lines in Zone 2 may display the name, address and other related information about the card. One great advantage of this primitive technology is that you can transfer the card details to paper without the need for power supply nor telephone line network.

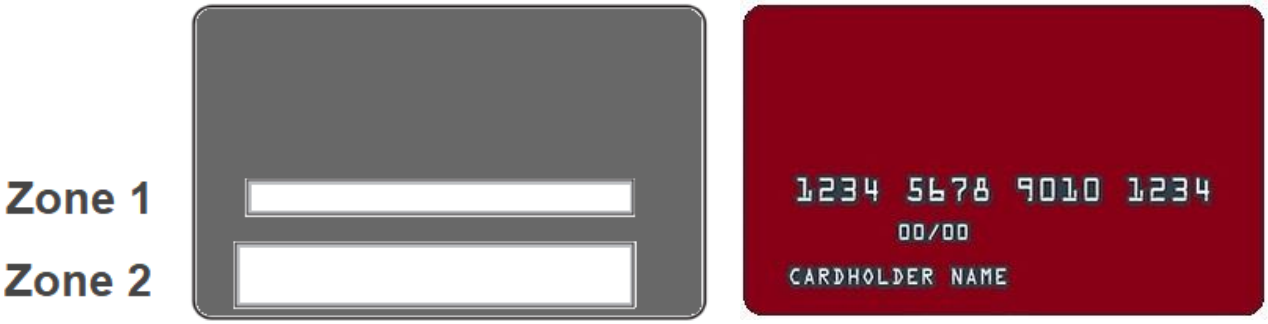


Figure 2 Embossed ID card showing Zones 1 and 2.

3. MAGNETIC-STRIPE CARDS

As mentioned previously, the embossed Identification cards advantage is that their data can be transferred to paper without the need for telephone network nor electric power. However, they have disadvantages as well, they produce massive piles of papers with data that need to transfer at later time, and this cost labor and time. The solution to this costly labour activity is offered by the introduction of Magnetic Stripe Cards.

Magnetic stripe cards maybe read by passing them across a magnetic read head. By moving the card near the reading head, the card data maybe read or written into the card, on the card magnetic area. However, the card data is susceptible to loss if it is nearby strong magnetic fields. To overcome this issue a strong coercive magnetic material coating is used and this may add cost to the card, or a

protective pocket is used to shield the card from nearby magnetic fields. The following magnetic stripe ID-1 card in Figure 3 shows three tracks, the first and second tracks are read only, while the third track is read and write.

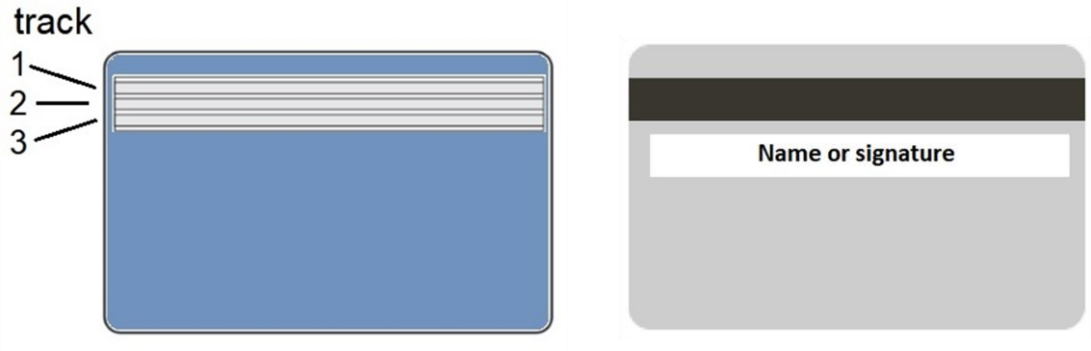


Figure 3 Magnetic card with three tracks, only the third track is read/write.

The magnetic stripe card can hold up to 1000 bits. All fixed data is kept in tracks 1 and 2, while updated data is written on track 3.

Magnetic stripe cards can be manipulated by learned people who have the skill of magnetic data manipulation. This manipulation imposes problems, specially to financial institutions who update the dollar figures on the card. The loss can be great when the wrong hands attempt such fraudulent manipulation. As mentioned before, only the third track can be written on and fraud attempt target this track. Once the data manipulation on the card is completed it is impossible for non trained personal to detect it and report it. Many attempts have been made to protect magnetic cards from fraud by adding sensors on checks and cards, this had increased the cost of the card manufacturing and thus was cost prohibitive.

4. SMART CARDS

So far, we have talked about embossed cards and magnetic stripe cards. Those cards have offered many advantages and disadvantages. There is a need for card security, larger data storage capability, ease of use, convenience and faster processing speed. Smart cards provide the above-mentioned needs at a very affordable card manufacturing cost. Smart cards have complex electronic circuit

buried inside them; it is called Application Specific Integrated Circuits (ASIC). This ASIC technology is embedded inside the card, it takes space much smaller than the card itself. Smart card ASICs receive data, process it, store it in card memory and then transmit it almost instantly and is highly reliable and secured. Smart cards can easily interact with card readers either by inserting them into the readers or by proximity of Smart card to the Card Reader. An electromagnetic or radio waves enable secure connection and communication between the Smart Card and the reader.

Smart card is a mini portable computer with the shape of card, most often the size of a credit card. Smart cards have no input or output devices such as keyboard and a display. Its shape factor allows smart card users to leverage the powerful mini smart computers without the need to carry with you large and heavy computer equipment. Smart cards get their power supply from the smart card reader, either by inserting them into the reader or by bringing them near the reader wireless power channel, also called wireless power zone. Today, there are near 50 billion smart cards being used in the World and trillions of dollars worth of transactions being performed by them. Smart cards have entered the government sectors and are used in health card electronic passport. Near 70% of smart cards issued in 2021 were contactless smart card that were used in various industries. By end of 2023, the smart card industry is expected to reach 22 billion dollars.

Smart cards can also accommodate the old features of Embossed cards and magnetic stripe cards, all in one hybrid card. This allows interoperability and back scaling between new technology with old readers, while enabling high level of cryptography and security for new card users. New smart card technology also has longer life span than the previous card technologies.

Based on the ISO/IEC7816 standards, smart cards are categorised based on the type of ASIC chip embedded inside them. Different chips deliver different features at different costs. The following image of Figure 4 depicts the grouping of cards based on the ASIC chips embedded inside them

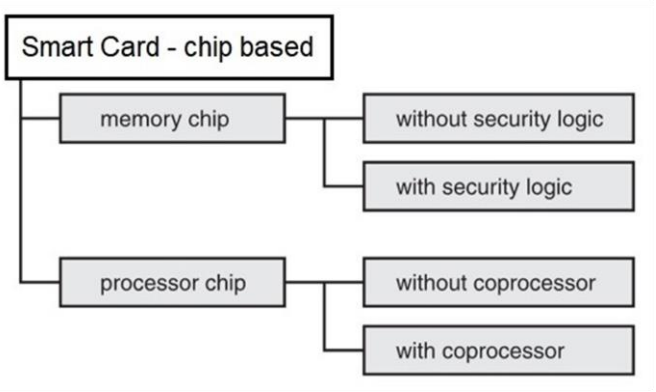


Figure 4 Grouping of smart cards based on the ASIC technology embedded inside them.

ISO standards also describe smart cards based on the method by which they communicate with the card terminal. Both the direct electric contact or contactless data communication methods can be implemented in the smart card as depicted in the Figure 5 below.

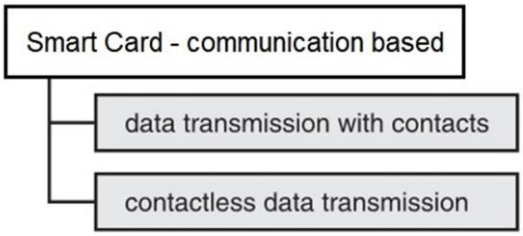


Figure 5 Grouping of smart cards based on the ASIC technology embedded inside them.

5. Contact Memory Cards

Memory based contact Smart Cards store important data and recall it upon request. Data is stored in permanent storage area called non-volatile, meaning that data stays in memory even after power is removed. Figure 6 below depicts a simple typical diagram of memory based smart card. Data flows in and out from the IO port, where IO stands for Input-Output. The access circuit allows intelligent addressing of EEPROM memory and it is secured via the embedded security

circuit and the ROM (Read Only Memory) memory stores fixed data. The communication between the card and the reading terminal is controlled via communication Clock and Enable ports. The Clock pin keeps data synchronised between the card and the reading terminal, and the Enable pin enables or disables the ASIC chip. ISO/IEC7816 defines how the smart card communicates with the terminal based on specific communication protocol that is available from a specific chip vendor. This Smart Card is perfect for low-cost applications that requires retaining user data such as driver license number or health card number in the ROM memory area.

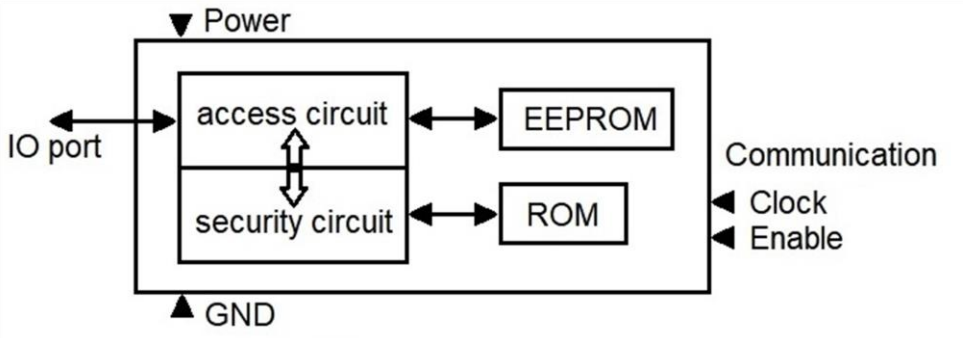


Figure 6 Simple typical diagram of memory based smart card.

In the following card of Figure 7, the electrical connections of embedded ASIC memory card are shown as per diagram of Figure 6 above. Depending on the design, the Power supplied from the card reader to the card could be 3.3 volts DC or 5 volts DC, IO is the pin that exchanges data between reader and the card and the Clock is used to sync data between the card memory chip and the card reader.

Figure 7 Electrical connections of embedded memory card.

6. Contactless Memory Cards

Contactless memory cards reduce, or eliminate, the mechanical parts involved in communicating with the card from the reader side. They can store up to few kilo bytes of data in them. The ISO/IEC14443 standard allows up to 10 cm distance to establish connection and reliable communication between the card and the reader. Contactless cards are passive, meaning they don't need battery to operate, they sniff power from the card reader. The ROM memory stores the fixed serial number that identifies and authenticates the user. The EEPROM may keep the code that process certain features on the memory card such as support for authentication and it can be updated externally to adapt to new requirements and to add more features and supports. The access circuit can reach the ROM and EEPROM memories via the wireless Interface circuit where it can read from and write to the EEPROM memory, but can only read data from inside the ROM memory. Figure 8 depicts a simplified architecture of the secured contactless Memory Card as follows:

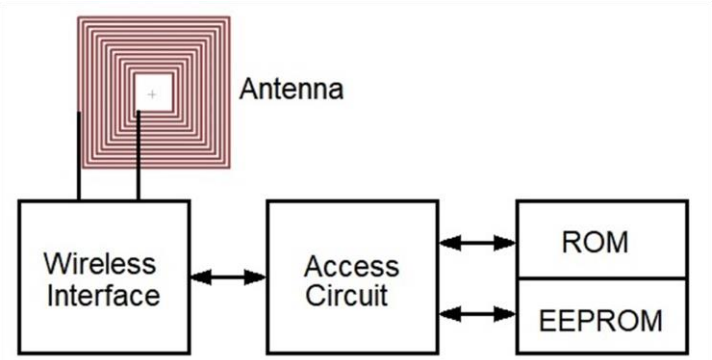


Figure 8 Shows simplified diagram for the secured wireless (contactless) memory card.

Contactless memory cards maybe used as access cards to identify employees entering secured area of the company. The company backbone software can identify the user from the employee ID number that is stored in the ROM. Those cards can also be used to give access to public vehicles or to the restaurant. Those cards can be made into a hybrid type of RFID and/or NFC cards that grant you the access rights to obtain a service or merchandise. Those cards are all assigned specifications and characteristics under the compliancy of the ISO/IE14443 standards.

7. Microcontroller / Processor cards

Before we start this section, lets understand what is the difference between microcontroller (MCU) and microprocessor (MPU). Both of MCU and MPU have a Central Processing Unit (CPU) that mainly performs the math and logic functions inside it. The MCU houses the CPU and support functions, called peripherals, inside the same silicon chip Integrated Circuit (IC). Peripherals may include features and functions of computer interface (such as USB), timers for timing events, Input and Output circuits, Data conversion circuits, memory and so on. On the other hand, the MPU houses a powerful CPU inside it, designers then connect this MPU to external Peripherals in order to deliver powerful and more advanced computing capabilities.

Application Specific Integrated Circuits (ASIC) is a technique used to house specific peripherals along with the CPU inside the same package. For example, you may have an ASIC chip that houses the CPU, memory and USB capability in one package. ASIC advancements allowed embedding specific mini-computers (microcontrollers) inside your smart mobile phone, smart wrist watch, remote control, vacuum cleaner, microwave oven, even inside your credit card and this is why it is called smart card.

Figure 9 shows the simplified structure of contact-based processor smart card. The CPU is linked to ROM, EEPROM and RAM memories all together. The CPU is also connected to the outside world via the Interface (Interface is usually implemented by serial UART or IIC communications protocol) and the Data pin (I/O). The smart card is powered up from the card reader after it is inserted in it. The Power (Power) is usually 3.3 VDC or 5 VDC, the ground pin is connected to GND, the Data pin is connected to the I/O pin, and the Data transfer and synchronisation is supervised by the Clock pin (CLK). The Reset pin (Reset) is used to perform certain CPU and reset functions.

Note that the left side of the Figure 9 below have 5 contact pins that electrically connect to the corresponding contacts on the pad to the right side of the Figure.

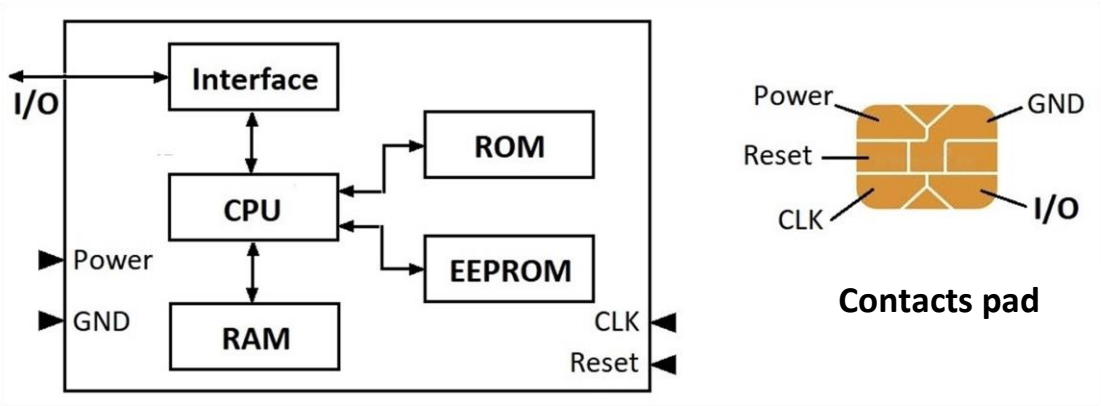


Figure 9 Contact processor card with memory and interface units. The processor electrical contacts are also mapped to the right of the figure, the contacts pad.

The EEPROM memory can be updated by memory writer device after it is inserted in the programmer or card reader. EEPROM is non-volatile, meaning its content will remain in the chip even after disconnecting the power of the card or programmer from the card reader. The ROM memory mainly has the smart card operating system written into during manufacturing and can not be changed after manufacturing. The RAM memory is used to perform data manipulation and management during the use of smart card, and its content will vanish after disconnecting the power from the smart card.

Smart cards can implement complex tasks by expanding their memory size and using more powerful peripherals, microprocessors or microcontrollers. The larger the memory size, the higher the processor speed, the more peripherals the smart card uses, the more power and capabilities the smart card can deliver.

8. Contactless processor cards

Today, you can tap your smart card over a smart card reader and instantly make a payment for your groceries or your new laptop. You may also enter your secured work place by taping your smart card (secured Identification card issued by your employer) into the reader and instantly get access to your secured office. All the authentication information is programmed into your smart card are handled securely and instantly without the need to inserting the card inside the reader nor having the security officer verify your identity. There are many other

similar applications that uses the smart card to make a secured transaction take place almost instantly. One of the forms of contactless smart card interaction with the reader is illustrated in Figure 10 below.

Figure 10 Contactless smart card is used to securely purchase merchandise from the market. The contactless card is tapped to the reader for instant purchase.

The term "contactless" refers to a breed of smart cards that uses a sort of wireless technology that operate over very short range of 10 cm or so. We use the term "contactless" instead of the word "wireless", because the second implies the use of battery and operating over a range farther than few centimeters. On the other hands, contactless smart cards do not use battery, instead they borrow power from the reader without physically contacting them.

There are advantages to using short range for contactless smart cards; they ensure that smart cards will not interact with the card reader if they are further than 10 cm away from the reader. Otherwise, a security issue and wrongful data collision, of many smart cards nearby the card reader, may impose many problems, leading to declining authentication and transaction. Data collision of smart cards will arise only if the reading range of contactless smart cards were longer than necessary.

Contactless smart card readers often have no moving parts and thus are harder to defeat and cause damage to them. They are faster, more reliable and safer to use than contact based smart cards. A wireless symbol is often used on the contactless card reader indicating that this area is where you should bring your card closer to it as shown in the Figure 11 below.

Figure 11 Wireless symbol is placed on the contactless smart card reader indicating compatibility and tapping area on the reader.

Contactless smart card can be used with old readers if the contact based electric contacts are added to the card, those "hybrid" cards allow the compatibility with wider range of card readers if certain segments of the market did not yet upgrade their Point Of Sale system, this hybrid card will keep business transactions up and running. A Dual-Interface hybrid card with three technologies combined together in one card; embossed card, contact based smart card and contactless smart card, is shown in Figure 12 below:

Figure 12 Dual-Interface Hybrid smart card can back scale from contactless to contact and embossed cards in one card.

This hybrid Dual-Interface smart card can have more advanced features integrated into it, depending on marketing, business and financial needs. More advanced smart cards are very convenient but come with added cost. The following diagram of Figure 13 depicts the simplified structure of the hybrid dual-interface smart card as described above. For more details about the block components, please refer to the previous sections about the contact-based microcontroller smart card and the contactless smart card.

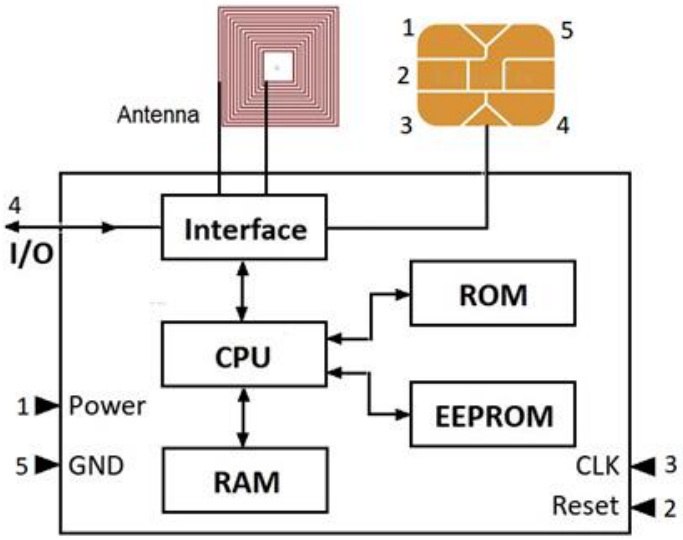


Figure 13 Hybrid Dual-Interface smart card with both the contact-based and contactless-based topologies embedded within the same smart card.

Note that the contact pad to the top right of Figure 13 above is segmented to 5 small contacts; 1 to 5. Those contacts are electrically connected to the smart of the card contacts labeled 1 to 5. Refer to the previous se3ctions for more details.

FT Automation is a Canadian company that designed a complete contactless based smart card system allowing you to capture the contact details of colleagues, professional contacts and friends in a split of a second. They designed smart card called system "Star" as shown in Figure 14 below.

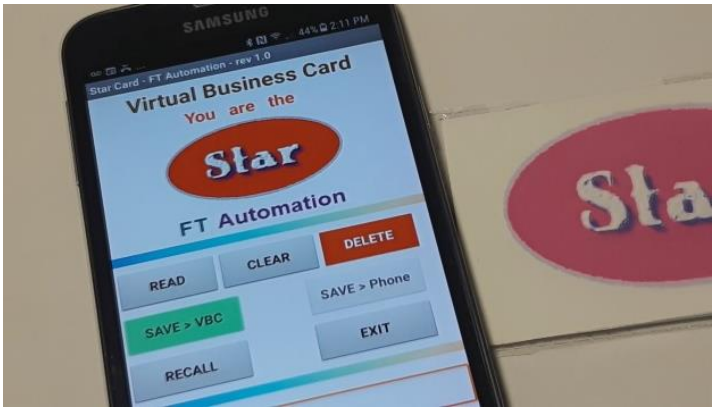


Figure 14 Contactless Smart Card App can capture any contact details in a split of a second, the Star. By FT Automation Canada.

The "Star" system is made up of the contactless smart card and an easy-to-use App that can identify and collect contacts of hundreds of people in very short period of time. This is a great time saving tool that transfers contact details accurately in split of a second. The company is located near GTA Toronto area and can deliver various services and products for your home and office automation.

You may download the free App from Google Play Store and get the feeling of the Star App. Visit the Star App at Google Play Store by scanning the following QR Barcode in Figure 15 below.

Figure 15 Barcode to download the "Star" App from Google Play Store and use with contactless Star smart card.

If you want to learn more about the "Star" contactless smart card then you may scan the following Barcode, in Figure 16, and link to the "Star" page.

Figure 16 Barcode to link to the "Star" page for more details about the Star contactless smart card and Star App.

2022

January

S	M	T	W	T	F	S
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

February

S	M	T	W	T	F	S
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	1	2	3	4	5

March

S	M	T	W	T	F	S
27	28	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2

April

S	M	T	W	T	F	S
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

May

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

June

S	M	T	W	T	F	S
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2

July

S	M	T	W	T	F	S
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

August

S	M	T	W	T	F	S
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3

September

S	M	T	W	T	F	S
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1

October

S	M	T	W	T	F	S
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

November

S	M	T	W	T	F	S
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3

December

S	M	T	W	T	F	S
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31