

# SMART CARDS

## Defining your Phone's PERSONALITY

By David Crowe

**T**he cell phones carried by about half of Canadians, and the vast majority of people outside Canada, contain a little chip, commonly called a 'smart card', that might be considered the brains of the phone. Although, perhaps it would be more accurate to call it the 'personality' of the phone. Quite easily removed, this chip can be transplanted into another phone, carrying your cell phone's personality with it.



Smart cards originated in the GSM (Global System for Mobile) standard that began as the first pan-European digital cellular standard in the early 1990s, but has since spread around the world, including, among others, Rogers in Canada, and T-Mobile and AT&T Wireless in the United States.

Originally, the SIM (Subscriber Identification Module) card, as a GSM smart card is known, was the size of a credit card so it could be slid into the side of early GSM brick-like phones. As the form factor of phones shrank dramatically in the 1990s, however, the size of the cards became a problem and the SIM card was reduced to the tiny 25mm x 15mm package (about 1 x 1.5 inches) that we know today. Well, that

you might know today. The smaller-sized SIM is cradled inside the phone in a special holder, often underneath the battery, so some people do not even realize that it is present. If you are not sure whether your phone has one, ask the closest teenager.

Other common varieties of Smart Cards are the USIM, which is adapted for UMTS/Wideband CDMA, the R-UIM (Removable User Identity Module) developed for cdma2000 and the ISIM for 'All-IP' systems.

Instead of special purpose smart cards, the current trend is to build support for a specific wireless protocol as an application on a generic smart card known as a UICC (Universal Integrated Circuit Card). This allows

the SIM, USIM, R-UIM and ISIM to co-exist as virtual smart cards (Master Files) on a single hardware platform.

**The smart card does not contain all the data and software for a phone, however it does contain the most critical data, as well as some other information that is handy to have on a removable card.**

### **Who Has A Smart Card?**

In Canada, smart cards are universal in GSM phones on both the 2G and 3G systems (using UMTS or W-CDMA) on the Rogers network. They are also found in iDen phones for the TELUS 'Mike' service and in the increasing number of phones supplied by the cdma2000 carriers that include a GSM module for international roaming.

What is less well known is that in many other countries, particularly in East Asia, these smart cards are almost universal, found in phones using all technologies, including cdma2000, which does not use smart cards at all in North America. In fact, a push known as the "Open Market Handset", originating with the carriers Tata and Reliance in India, is an attempt to provide an extremely cheap and generic phone which would have all of its personality and carrier branding defined by the smart card. This illustrates a completely different business model than in Canada. Carriers in less wealthy countries rely less on glossy stores where high-end models are spotlighted to tempt consumers. They are less concerned with upselling phones to consumers, but rather more simply focused on getting them started on service. If an ultra-cheap unbranded phone will increase sales of branded smart cards and thus airtime, then the carriers are happy.

### **The Core of a Smart Card**

The smart card, of whichever type, does not contain all the data and software for a phone, however it does contain the most critical data, as well as some other information that is handy to have on a removable card. The card contains the identification of a subscription, provides secret authentication data and usually also some storage for phone numbers, text messages and even applications and multi-media messages, depending on the memory size of the card.

Identification in telecommunications usually implies numbers, and the SIM card has several: one to identify the card, one to identify the subscription and one for the subscriber's phone number.

The card identity is known as the ICCID (International Telecommunication Charge Card ID), and it is easily recognized because it always starts with '89' followed by the country code of the carrier and then a long serial number. In total, the number is 19-digits long, with the last digit being a 'check digit' calculated using the Luhn algorithm that can detect most simple input errors. You may see this number printed on the smart card itself (in very small print, so here again, a teenager may come in handy).

Much more important than the ICCID, particularly after a card has been registered with a wireless carrier, is the MIN or IMSI, a number that uniquely identifies a subscription on a wireless network. Every time a phone accesses the wireless network, or the wireless network attempts to contact the phone, this number, or a surrogate directly tied to it, is transmitted.

Lastly, the card may contain the mobile's phone number. This is not used by the system, but is only provided for the user's information. It is helpful that when someone asks their phone for their phone number, it provides the phone number, and not the MIN or IMSI, which might mean nothing to them.

In addition to telecommunications identifiers, packet data identifiers may also be stored, often in the form of a username and password.

It is not common today, but it is theoretically possible to start with a card with only the ICCID, and to provision all other identifiers when the subscriber first inserts it in a phone. This would dramatically simplify the management of card inventories for carriers with large national networks because the IMSI, MIN and phone number are often assigned regionally. Making these assignments at the time the card is initially provisioned means that all cards are identical and thus can be shipped anywhere. This capability requires access to the ICCID over the provisioning interface (something that is not always available) and also a database that connects the ICCID to security data, an initial prepaid balance and other characteristics.

### **Under the Hood**

The smart card, despite its tiny size, is very sophisticated. Most contain at least three types of memory: ROM and RAM to support the embedded operating system, and EEPROM where the user's files are stored. The smallest and cheapest cards have 16K EEPROM, but the largest hold up to a Gigabyte.

This memory is organized into a simple three-level file system with individual files identified numerically. This might sound unfriendly, as most modern file systems allow named files and many levels of nesting within the file system. However, since the files are only accessed by the phone's software and not directly by the user, this is not a problem in practice.

In fact, even the word 'file' is a bit misleading. Many of the files are tiny and contain individual data components, such as an IMSI or ICCID, and thus are often only a few bytes long, unlike the much bigger and more complex files we are used to on a general purpose computer.

Managing the file system, communicating with the host phone, and other operations are managed by a simple operating system on the card in the ROM and RAM that are provided.

Next to the amount of memory available, the speed of accessing

it is the next most important characteristic. Having a huge amount of memory on a device with a low speed interface is futile, because the pipe is too thin to get the data in and out in a reasonable amount of time. Current smart cards are driven by an external clock which the phone and card can negotiate to run at clock speeds between 1 and 5 MHz. A much faster interface, based on USB and providing full USB 2.0 speed – 480 Mbps – has been standardized by ETSI. When widely implemented, it is safe to predict that the size of smart cards will climb aggressively.

## **Having a huge amount of memory on a device with a low speed interface is futile, because the pipe is too thin to get the data in and out in a reasonable amount of time.**

### **Security**

Next to identification, security is probably the most important function of these cards. In fact, identification without security is futile because the identification cannot be verified.

Security requires a seemingly strange type of file – one that is not accessible at all. Well, the files containing security algorithms are accessible, but only from within the card. The files are completely inaccessible to any communications via the external leads, whether the card is inserted into a phone or a card reader.

The basic security required for wireless communications is authentication, which is a technique to prove that someone is who they say they are. In the context of MIN or IMSI, authentication proves that the smart card is the one that the legitimate subscriber purchased. Without

authentication, the MIN or IMSI can be ‘cloned’ – something that defrauded cellular carriers of hundreds of millions of dollars in the bad old days of the early 1990s.

Authentication is usually based on a “Challenge–Response” algorithm. The network picks a large random number and sends it to the phone which sends it to the R-UIM where a cryptographic algorithm is executed, taking the random challenge and the heavily secured secret key, along with some other information, to produce a response. Given the output, and even knowing some of the inputs, the secret key cannot be derived in any reasonable amount of time. The R-UIM provides the response to the phone which transmits it back to the network. If the network has calculated the same response, the mobile/R-UIM combination is authenticated, and service can be provided based on the characteristics of the subscription or pre-paid account identified by the MIN, IMSI or packet data identification.

Other important security algorithms include the encryption of voice and data communications. Wireless communications systems generally do not provide end-to-end security (often this is impossible), but do secure the radio interface, eliminating the possibility of eavesdropping.

Another type of security is “integrity checking”, which uses an encrypted checksum on each message to verify that the contents have not been tampered with (even unencrypted parts).

All of this is unlocked by a user by entering the PIN for a smart card before it allows the phone access to its security capabilities. Consequently, the longer the PIN the better. If the PIN of a stolen smart card can be guessed easily, then all security on the smart card is bypassed at least temporarily. If the worst happens, the subscription can simply be disabled once a lost card is reported until it can be associated with a new smart card.

One of the downsides of smart cards is that it is easier to use a stolen phone because the smart card can simply be discarded. Because of this, some carriers implement an EIR (Equipment Identity Register) that can look at the phone’s unique identity and prevent stolen phones from being used even with a legitimate smart card.

### **Bells and Whistles, Photos and Games**

If there is enough memory on the card, more advanced functions can be provided. Storing non-essential information on the card means that you can easily take it with you when you change phones temporarily or permanently.

Storing SMS text messages and a phone book were some of the earliest smart card applications, but now many more are available.

Java applications are possible on cards with more than the basic 16k of memory. Java can include games, instant messaging, Web browsers, mobile banking, calendars and e-mail. Most importantly, these can be provided by third parties, encouraging innovation and niche applications.

Some of the bigger cards have the bulk of their EEPROM acting as a memory card for photographs, multimedia messages and so on. This can be accessed like a normal plug-in memory card, but with the added benefit of the security provided by the smart card. In other words, if the memory card falls into someone else’s hands, it cannot be accessed unless the PIN for the smart card is known.

### **Paying the Piper**

Smart cards can be purchased from many operators as either prepaid or postpaid. A prepaid card does not actually carry any information about the amount of money associated with it, but the subscriber’s identity, once authenticated, is the key to a network database containing the prepaid balance. Most prepaid systems

allow for funds to be added to the account, so the prepaid smart card can be used indefinitely. This can be done in a number of ways: through a Web interface, through the phone itself, or by buying a scratch card, particularly in cash-based economies.

Postpaid accounts are those that Canadians are most familiar with, where call charges are billed monthly. This method is less common in countries where people might not have the credit required by the carrier to assure them that payments are likely to be made each month.

### On the Horizon

One of the long term aims for smart cards has long been for them to be used for both communications and banking, rather than requiring two separate devices. To accomplish this, carriers will have to develop a strategy, sign business agreements and solve technical problems. Unless a carrier wants to also become a bank or credit card company, they will have to find partners in this sector. They can choose to sign an exclusive arrangement with one bank, but not all customers would appreciate the lack of choice this would imply. Or they could try to be simply a broker for banking and credit card services, allowing customers to choose any service that had the technical requirements. Another alternative would be to sell smart cards with a blank area where banking capabilities can be provisioned and secured by a third party. Europe and Asia are definitely more advanced than North America in this area.

To make the use of a phone for payment easier, 'contactless' payment can be implemented. This requires a CLF (a Contact-Less Frontend that operates by NFC – Near Field Communications, essentially an RFID tag) within the phone that can communicate with

the smart card to perform a security transaction with the financial system over a very short distance. The user just 'swipes' the phone within a few centimeters of the payment device and then enters a PIN to ensure that the payment is authorized. Developments in this area are quite recent, and rely on the SWP (Single Wire Protocol), a series of ETSI standards that connects the CLF to the smart card at several protocol layers.

Phones in Canada work with or without smart cards today, but as the applications and capabilities grow, it is likely that a significantly larger fraction will use them in the future. ■

*David Crowe is a wireless standards, technology and numbering resource consultant based in Calgary. He can be reached at David.Crowe@cnp-wireless.com.*

**Cardo, Setting the New Standard for Bluetooth® Headsets**

**CARDO**  
CARDIO SYSTEMS, INC.

**The Cardo S-800™**

**The Perfect Combination of Precision Design and Advanced Headset Technology.**

The superbly styled S-800 offers access to you favorite three numbers with one-touch Hot Dialing, SWAP Technology to switch between two mobile phones, and a unique headset location buzzer to find the headset if misplaced.

**scala-700LX™**

Setting a new standard for Bluetooth® headsets

- **SWAP Technology:** Switch between two mobile phones with a touch of a button.
- **Headset Location Buzzer**
- **Missed-call Indicator and Call-back Function**

Auto Answer, Conference Call and more...

**The Cardo S-2™** Provides wireless hi-fi stereo and allows hands-free voice control of your mobile phone and MP3 Player all in one product

**Wireless Stereo Headphones with Advanced Function and Hip Retro Design**

**HITFAR**  
www.hitfar.com  
1.800.661.1186  
604.873.8355