How do Smart Cards Work

Definition:

A **smart card** is a credit card device that includes an embedded integrated circuit (SMART CHIP) that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone.

The **card** connects to a reader with direct physical contact or with a remote contactless radio frequency interface. The Radio Frequency ID (RFID) is unique for each smart card application (like radio stations over a spectrum) and is used as a carrier for digital data communications like a modem would be in a communications system. The smart card communications is also based on Carrier Sensing Collision Detection (CSCD) technology protocols that sense the carrier frequency to match its speed, and when two-way communications is used collisions are detected and retransmission performed based on priority of direction (usually receive is higher than transmit because you already know what you are transmitting, but don't know what you are receiving yet).

Smart Cards cannot provide GPS services, which require a power source to support continuous operation not fond on any current smart cards, but an audit trail can be used for tracking where an individual uses their card.

Smart Card Chip

A smart card resembles a credit card in size and shape, but inside it is completely different. First of all, it *has* an inside -- a normal credit card is a simple piece of plastic. The inside of a smart card usually contains an **embedded microprocessor**. The microprocessor is under a gold contact pad on one side of the card. Think of the microprocessor as *replacing* the usual magnetic stripe on a credit card or debit card.

Smart cards are much more popular in Europe than in the United States. In Europe, the health insurance and banking industries use smart cards extensively. *Every* German citizen has a smart card for health insurance. Even though smart cards have been around in their modern form for at least a decade, they are just starting to take off in the United States.

Magnetic stripe technology remains in wide use in the United States. However, the data on the stripe can easily be Created, Read, Updated, or Deleted (CRUD) with off-the-shelf equipment. Therefore, the stripe is really not the best place to store sensitive information. To protect the consumer, businesses in the U.S. have invested in extensive online mainframe-based computer networks for verification and processing. In Europe, such an infrastructure did not develop -- instead, the card carries the intelligence.

The microprocessor on the smart card is there for **security**. The host computer and card reader actually "talk" to the microprocessor. The microprocessor enforces access to the data on the card. If the host computer Created or Read the smart card's random access memory (**RAM**), it would be no different than a **diskette**.

Smarts cards may have up to 8 **kilobytes** of RAM, 346 kilobytes of **ROM**, 256 kilobytes of programmable ROM, and a 16-bit microprocessor. The smart card uses a serial interface and receives its power from external sources like a card reader. The processor uses a limited instruction set for applications such as cryptography.

The most common smart card applications are:

- Credit cards
- Electronic cash
- Computer security systems
- Wireless communication
- Loyalty systems (like frequent flyer points)
- Banking
- Satellite TV
- Government identification

We have realized that there are many other uses for Smart Cards, starting with proving that the card holder is who they claim to be by utilizing the individual's bio-metric information (eye scan, facial recognition, finger print, palm print, or even DNA analysis information) along with the individual's name and contact information. Any application or service that is based on an

individual's proven identify could use this smart card to allow the individual to gain access to their secure environment. Now we are introducing the capability of using bio-metrics in smart cards to support additional applications for:

- Voter ID Cards (***eCARD*** containing voter bio-metric information to validate identity)
- Electronic Voting Systems (***eVOTE***) to guaranty "One Person-One Vote" and to eliminate voting Fraud and Corruption.
- Medical ID Cards (***eCARD*** variant DNA, Medical, Biological, Chemical data) to support patient treatment tolerance and provide access to HIPAA patient history.
- Electronic Medical Assistant (***eMEDICAL***) applications when an accident occurs away from home and Emergency Medical Technicians and Emergency Room Physicians need to have immediate access to your medical information to provide quality treatment without the threat of providing a drug you are allergic to or when determining correct dosages.
- ***eCARD APPS*** can be used to support other uses for smart cards like personnel Vetting (***eVETTING***) and **Real ID Act** compliance (***eCARD APP***)

Smart cards can be used with a smart-card reader attachment to a **personal computer** or hand held **smart phone** to authenticate a user (think IPhone or Apple Square). Web browsers also can use smart card technology to supplement Secure Sockets Layer (SSL) for improved security of Internet transactions, which may someday support remote voting from your home.

An example of how Smart Cards work with new credit cards

Smart Card FAQ describe how online purchases work using a smart card and a PC equipped with a smart-card reader. Smart-card readers can also be found in **mobile phones** and vending machines.

Smart Charge Card Uses

Smart Charge Card chips are not only more secure, they are also simple to use. Chip cards and terminals work together to protect in-store payments. A unique one-time code is generated behind-the-scenes that is needed for the transaction to be approved - a feature that is virtually impossible to replicate in a counterfeit card. This feature is dual password authentication because first you provide your known password and when recognized then a second password generated by the receiver, downloaded to your smart card, and then read from the smart card back to the receiver is used to authenticate your identity.

To initiate a transaction, the smart card is inserted into the receiver and will remain in the receiver throughout the transaction. The card reader will send power to the smart card so that

the reader can read the smart card information and use it to compare against your entered PIN. Then the dual authentication process is initiated and completed to guaranty the card and its user are indeed an authorized card holder. The transaction is initiated and completed, with the card holder responding to requests for information (PIN, amount approval, etc.) and the information provided to the vendor and payment made. Throughout this process, the smart card is retained in the card reader slot, which is a feature we use in our electronic voting system (***eVOTE***).

The eVOTE electronic voting system is based on "One Person – One Vote", so validating that a person is who they claim to be is our initial challenge. We do this through a data base structure that uses a Parent Record to identify the individual's name and contact information, and a Child Record to store the individual's bio-metric information. We call this process "Personal Verification", but we do not stop there. When the individual's smart card (Voter ID Card) is read, the information is passed to our Registered Voter Data Base and compared with the individual's information. If a match is NOT made, then we assume the individual is NOT who they claim to be. We retain the card in the reader and notify the guard at the Voting Station of the event. The guard can then detain the individual and the fraudulent card for questioning and possible arrest, thereby nipping voter fraud in the bud. If a match IS made, then we take another step by comparing the individual's information against the "Active Voting Data Base" to see if the individual has already voted in this election at a different location (Personal Validation). Again, the guard is notified and the individual is detained (along with the card) for questioning and possible arrest.

Our system also has the ability to compare the Voter ID information against other data base system to prove that the person is allowed to vote and not a felon or in another category that would stop them from voting.

Providing information to support criminal investigations and prosecution

The eVOTE electronic voting system has been designed to capture vital information every step of the process it uses to create a Voter ID Card through the verification and validation process to when a voter enters the voting booth and casts their ballot. This information includes:

1. The individuals name and contact information,
2. The Individuals bio-metric information,
3. Creation of the Voter ID Card and tracking it back to the original stock number,
4. Voter Verification and Validation,
5. Voter ballot selection (including language selection and instruction review),
6. Services provided to handicapped individuals.
7. Even pictures taken when the voter submits their ballot,
8. Time and Date Stamps all along the process.

9. Maintenance of a Voter Activity data base during the election, and
10. The archiving of the Voter Activity Data Base when an election is completed, so that future investigations can have access to this information.

This information, along with the associated Audit Trail (or Trail of Evidence to those of you in law enforcement) can be used to prosecute voting fraud and corruption cases in a much more efficient manner than is experienced today where many offenders get off without charges due to lack of evidence.

Using a Smart Card for a transaction

Step 1

Insert the chip end of your card into the terminal (instead of swiping).

Step 2

Keep your card in the terminal to complete your purchase until the terminal prompts you to remove the card.

Step 3

Don't forget to take your card with you when you leave

An important issue to remember is that the card is retained in the machine until the operation is completed. There are various types of card readers, but they provide the power to the smart card via gold contacts and Radio Frequency transmissions (RFID)

As merchants adopt Smart Charge Card chip technology, there are a few things to keep in mind:

- Larger merchants will be among the first to deploy chip-activated terminals, with more merchants deploying over the next few years
- You can still swipe your chip-enabled card using the magnetic stripe on the back of the card at merchants who haven't yet updated their terminals
- When you swipe your chip-enabled card at a chip-activated terminal, the terminal will prompt you to insert the card into the chip slot instead
- Use your card for payment over-the-phone or online just like you always have
- Insert or swipe — you're always protected from unauthorized transactions with a **Zero Liability Policy**.

Preferred in more places

You can use your smart chip card anywhere it is accepted because the chip card offers additional benefits:

- When you travel internationally, transactions that strongly prefer chip cards will be simple and secure
- Chip technology helps pave the way for innovations like mobile commerce, helping to ensure that wherever and however you want to pay in the future is secure and convenient

Enhanced security

In addition to creating unique codes for every transaction, smart cards can also provide security by:

- Protecting against fraud through guarantying personnel identity

- Performing Local Verifications of a person's identity and remote Validation that the person has not committed a crime like trying to vote twice in a single election.
- Double authentication for individual cards.
- Unique RFIDs for each card type and vendor issuing the card.

In essence, the use of Smart Card technology will increase over time because the technology will follow the three phase growth path that other widely accepted technologies have experienced, which is:

1. Produce usage and acceptance.
2. Rampant growth,
3. Management of the resource through efficiency and cost controls.

Where do we go from here?

It is easy to realize that Smart Card technology can be used in conjunction with a variety of services and products where it is essential to authenticate the user is who they claim to be. For this reason, smart card growth will be associated with some of the following services and products as smart card applications (***eCARD APP***):

1. As a Universal Smart Card that can be used for many applications.
2. To maintain and individual's Name and Contact information, should they move, where one card can access all of the services and products used by the individual to maintain their contact information for mailing and billings.
3. To adhere to the Real ID Act of 2005 where all states must provide compliance or their citizens will be denied access to sensitive services, like domestic air travel.
4. To comply with the Patriot Act's clause of Know the Customer.
5. As an aid to law enforcement for vetting individuals and locating criminal suspects.
6. As an aid to the Justice and State departments in support of FBI and CIA activities.
7. In the healthcare industry to provide emergency medical information.
8. As an aid to individuals who want access to their HIPAA information in a single data base that can provide history and current medical information necessary to receiving optimum medical treatment with minimal chances of drug reactions due to drug tolerance, combinations, and dosage guidelines.
9. DNA Analysis for family history and medical guidance.
10. In support of a cashless society going forward.

This small list of possible uses, if implemented, can change society forever. For example, with a cashless society theft would be eliminated because there is no money to steal and stealing the smart card would do a criminal no good because they could not use it. Adherence to government regulations and laws would be much easier. Tracking felons and suspects can be

easier. Vetting individuals (***eVETTING***) would be easier because of the bio-metric identification and access to various data bases in America and abroad. A World-Wide network of individual identity data bases could be connected to protect society and a countries borders.

Contacting me

I am devoted to this technology and its implementation because I believe it will have a positive impact on society and I also believe a lot of money can be made by its implementation.

Should you have questions, or want to make recommendations for improvement to this article, then I can be reached via email at bronackt@gmail.com.