



WP118 (v1.0) May 18, 2000

Using CoolRunner CPLDs in Smart Card Reader Applications

Author: Karen Parnell

Summary

This document presents the different types of smart cards and their applications and discusses the variety of smart card readers available and what functions they can perform. An illustration of the elements that form a typical smart card reader and how and where CoolRunner devices can be used to undertake some of these tasks is described herein.

Introduction

Smart cards and smart card readers are becoming a common part of our every day lives, and their usage will rise as new ways to use this stored data and processing power increases. Xilinx high-volume programmable devices can be used to implement various functions within smart card reader designs and are particularly beneficial in their hand-held, lightweight, battery powered versions. Xilinx devices targeted at this high-volume application are the latest family of ultra low-power devices—CoolRunner CPLDs.

CoolRunner CPLDs are ideal in such applications as portable smart card readers because they benefit from total CMOS Fast Zero Power (FZP™) design technology that combines low power and high speed. CoolRunner CPLDs are available in extremely small form factor packages (Chip Scale Ball Grid Array) which allows smaller and lighter designs.

Smart Card Market Overview

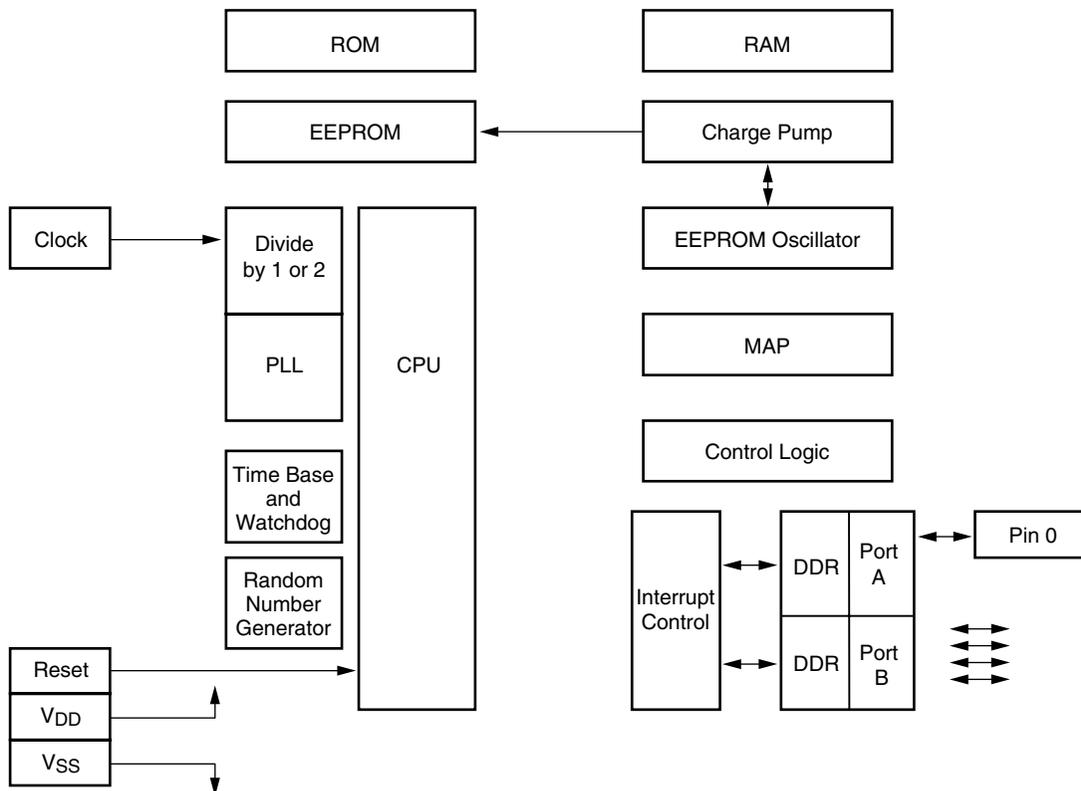
Imagine a time when we go to get our morning paper we could simply use a card charged with small denominations of money to pay for the paper instead of fumbling for small coins. When we rush to get on the bus we simply use the same card to pay for the ride. After arriving at work we then take out the card and unlock the security door and enter the office. Once at our desk we insert the card into a reader on our PC and the computer boots up into our own personal configuration. While at the computer we decide to pay for a subscription to our favorite club by entering their website, the card is then interrogated for club membership details and then the exact amount is debited from our account using the on-card bank details. Imagine replacing all of the cards and cash in your purse or wallet with just one card. It may seem far-fetched but with the rapid advancements of semiconductor technology this type of card is a reality. In some parts of the world the "smart card" has completely replaced the magnetic strip card.

Why is the smart card replacing the magnetic strip card? The main reason is that the smart card can hold up to a 100 times more information than a traditional magnetic strip card. The smart card is classed as an integrated circuit (IC) card. There are actually two types of IC cards: memory cards and smart cards. Memory cards contain a memory device that allows the card to store various types of data. However, they do not have the ability to manipulate this data. A typical application for memory type cards is a prepaid telephone card. These cards hold typically between 1Kb and 4Kb of data.

A memory card becomes a smart card with the addition of a microprocessor. The key advantage of smart cards is that they are easy to use, convenient and can be used in several applications. They provide benefits to both consumers and merchants in many different industries by making data portable, secure, and convenient to access.

Inside the Smart Card

A smart card is very similar in appearance to an ordinary credit card but with the addition of embedded ICs (memory and microcontroller) and contacts for the ICs on one side. The smart card may also include a magnetic strip for conventional transactions. The embedded microcontroller allows the card to make computations, decisions and manipulate data, in other words, this is the "smart" part of the card. Figure 1 shows a block diagram of the smart card internal circuitry.



Source: IEEE Spectrum

WP118_01_051700

Figure 1: Block Diagram of Smart Card Circuitry

A typical smart card consists of an 8-bit microcontroller (MCU), 16Kb of ROM, 512 bytes of RAM and up to 16Kb EEPROM or flash memory all on a single device. There are many types of memory within the card—RAM for temporary data storage, which is only used when power is applied (usually when the card is in contact with the reader) and ROM which stores fixed data and the operating system. The use of nonvolatile memory such as EEPROM or Flash memory is ideal for storing data that changes such as an account PIN or transaction data, the type of data that must remain stored once the power is removed.

Manufacturers of smart cards are moving to a 32-bit microprocessor in order to increase processing power and handle more applications.

Within the umbrella term "smart card" there are a two main types:

- Contact smart cards: these require insertion into a smart card reader
- Contactless smart cards: require only close proximity to an antenna

The contact smart card has a small gold chip about ½" in diameter on the front, instead of a magnetic strip on the back like a credit card. When the card is inserted into a smart card reader, it makes contact with the electrical connectors that can read information from the chip and write to the chip.

A contactless smart card looks just like a typical credit card with a microprocessor and an antenna coil inside, which allows it to communicate with an external antenna. Contactless smart cards are used when transactions must be processed quickly, as in mass-transit toll collection.

The "combicard" is a single card, which functions both as a contact and contactless card.

Here are some advantages of the smart card over the traditional magnetic strip card:

- Proven to be more reliable than the magnetic strip card
- Can store up to 100 times more information than the magnetic strip card
- Reduces tampering and counterfeiting through high security mechanisms
- Can be reusable
- They have a wide range of applications (e.g., banking, transportation, health care, etc.)
- Compatible with portable electronics (e.g., PCs, telephones, PDAs, etc.)
- Cards can store many types of information—finger print data, credit, debit and loyalty card details, self authorization data, access control information, etc.

History of Smart Cards

The development of smart cards started in the 1970s with the first "smart card" being produced in 1977. Bull CP8 and Motorola developed the first card; it was a two-chip solution consisting of a microcontroller and a memory device. Motorola went on to produce a single chip card called the SPOM 01.

The use of smart cards have grown at a phenomenal rate in Europe by replacing traditional credit cards. The key to the success of smart cards in this area has been the ability to authorize transactions "off-line", i.e., the smart card stores the "charge" of cash enabling a purchase to be made up to the amount of money stored in the card. Motorola's single chip solution was quickly accepted into the French banking system. It served as a means of storing the cardholder's account number and personal identification numbers (PIN) as well as transaction details. By 1993, the French banking industry completely replaced all bankcards with smart cards.

In 1989, Bull CP8 licensed its smart card technology for use outside the French banking system. The technology was then incorporated into a variety of applications such as Subscriber Identification Modules (SIM cards) in GSM digital mobile phones.

In 1996 the first combined modem and smart card reader was introduced. We will soon see the first generation of computers delivered with the capacity to read smart cards as the standard.

In May 1996, five major companies in the computing industry (IBM, Apple, Oracle, Netscape and Sun) have proposed a standard for a new form of computer called the "network computer". The network computers are designed to interface directly with the Internet and have the ability to use smart cards. Also in 1996 the alliance between Hewlett Packard, Informix and Gemplus was launched to develop and promote the use of smart cards for payment and security on all open networks.

Besides using smart cards for e-commerce, there are endless possibilities:

- Carrying your favorite addresses from your own personal computer to your friends network computer,
- Downloading your airline ticket and boarding pass,
- Booking facilities and appointments via websites, and
- Storing log-on information for using any work computer or terminal, etc.

Smart Card Market Potential

Smart card usage worldwide is increasing at an extraordinary rate (Figure 2). Dataquest predicts that by the end of the year 2000 there will be 2 billion units in circulation. A leading smart card reader manufacturer (Gemplus) predicts that by the year 2018 there will be 5 billion phone cards alone, this does not include smart cards used for medical records, personal ID, loyalty cards, etc. All of these smart cards in circulation require smart card readers.

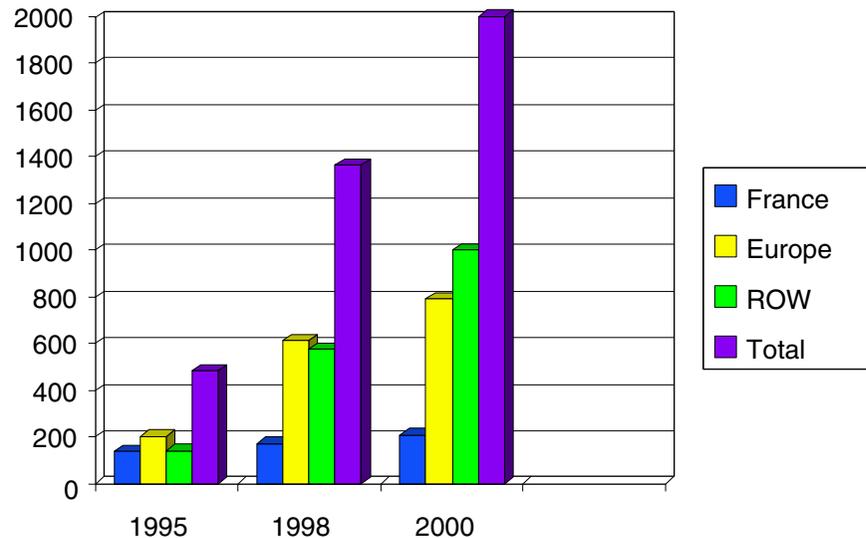


Figure 2: Smart Card Usage up to the Year 2000 in Million Units.
Source: Philips Communication Systems

To date Europe has dominated the smart card industry both in production and usage (see Figure 2). The region produces as much as 90 percent of the world's smart cards and consumes about two thirds. Europe's share of the smart card market has been declining, however, as the cards have started gaining popularity in other parts of the world. By the end of the decade smart card usage is expected to be evenly split between the regions—Europe, the Americas, and Asia.

One of the major long-term successes in the US has been college campus smart cards. These multi-application smart card systems provide students with services such as ID, parking, ATM access, library check out, dormitory access and payment services at vending machines, laundry, telephones, and book stores. Since 1996, the number of students carrying smart cards in the US has grown to more than 1 million, a number that represents approximately 1 in 17 students. This growth in campus cards is producing a generation of people who already understand the many benefits of smart card technology and therefore they may be more inclined to use them in larger, open system applications.

Smart Card Applications

Smart cards are being used in a number of applications ranging from stored value cards (SVCs) to transportation, medical and identification cards. As they become cheaper to produce, disposable smart cards will become available alongside long-term use cards, such as multi-function credit cards. The low-cost disposable smart card will become common place in applications such as one-day travel cards, flight tickets and even concert tickets. The following are a few of the many ways smart cards are being used today; application areas are increasing daily in this rapidly growing area.

- **Stored Value Cards (SVCs).** SVCs also known as electronic purses are being championed by companies such as Mondex International (Mondex), Banksys (Proton) and Chipper International (Chipper). These cards allow small denominations of money to be stored on the card in various currencies if required. The SVCs can be used for small value purchases where it is inappropriate to use a credit card. The SVC needs to be "charged"

with cash and as each transaction is completed the appropriate amount is deducted until the card is empty. Some companies are producing small key ring type readers with a small display, which can read the amount left on a SVC.

For example, a single card could be used as a credit card, debit card, SVC, access card, video rental card and medical record file. Other applications for SVCs include vending machines, parking meters, pay TV, cinemas and convenience stores.

- **Phone Cards.** Public payphones are moving towards having the coin slot replaced by a smart-card reader. The benefit of using smart cards to pay for calls is two fold—the user cuts down on cash carrying and the telephone company benefits from the elimination of theft. This type of stored value card counts down the money spent on each call and can be either recharged or disposed of.
- **Health Care Cards.** Health care cards are used to store pertinent information about the cardholder's doctor, blood type, allergic reactions, medications, next of kin, emergency telephone numbers and other health details such as dental records and private health card details. Planned and historical visits to the dentist and the doctor can also be stored and updated on the card. This type has proved to be very popular in Germany with most of the population carrying such a card.
- **Transportation Cards.** It is estimated that worldwide there are 20 billion commuter transactions. All of these transactions take time, hence the move towards smart card technology and especially contactless transactions. This would mean the time taken to pay for a ticket for, say, a subway train, and then pass through a security barrier would be drastically reduced. For example, as a person passes through a turnstile, he or she could hold their card in close proximity to the reader and the card would be read, money deducted and the barrier opened.
- **Prepay Utility Meter Cards.** These type of cards are very popular in regions where there are a lot of seasonal worker movement or short term tenant agreements and ensures that utilities such as water, electricity and gas are paid for in advance or "pay as you go". The card is "charged" with money and then inserted into the utility card reader and money deducted to allow a certain amount of gas, electricity or water to be used. The meter usually shows as a count down of how much fuel is left. This type of utility payment has proved very popular in South Africa.
- **Personal ATM.** Public and private telephones and PCs with smart card readers could make personal ATMs possible. This would allow users to load funds onto your smart card from your bank account or to top up the limit of a pre-authorized debit card. Financial institutions can make these facilities available wherever there is a phone—without the need for costly traditional ATMs. These telephone transactions can allow funds to be transferred from person to retailer, bank to account holder and even person to person.

Smart Card System Architecture

The complete smart card system includes the card, the card reader and the operating software. The smart card contains the appropriate ICs to store and manipulate data. When the card is inserted into the reader, the reader communicates with the smart card MCU to perform authentication functions. The card then performs the requested function, such as a deduction of a stored value. When the transaction is complete the card is then removed. The reader is now ready to accept the next card transaction.

The interaction between the card and the card reader is where standardization plays such an important role. For example, the idea that consumers would have to carry one smart card for each of several different merchants that they purchase from is inefficient. Already consumers carry several different cards ranging from video rental cards to discount shopping cards to credit and debit cards. Standardization in cards and card readers would allow for one card to be accepted and read by different readers.

The key to multi-application cards is multifunctional operating systems to avoid interference with each program. JavaCard (Sun Microsystems) and MULTOS™ are two operating systems that let cards perform multiple functions. Some companies support Java and some support

Multos but fortunately for users these are compatible with each other. Another provider of OS software for smart cards is Microsoft Smart Card for Windows.

MULTOS is a multi-application operating system for smart cards; the MAOSCO consortium controls its specifications. The main elements of the MULTOS architecture are a virtual machine (MEL interpreter) and an application loader. Smart card applications are coded in MEL (MULTOS Executable Language) and are hardware independent. In contrast to the JavaCard, the MULTOS virtual machine (VM) is completely realized inside the card. Generally there is a distinction between off card and on card VMs. MULTOS offers a 100% on card VM with firewalls between the applications. With this design, MULTOS meets the highest security criteria.

The application loader ensures secure loading and deletion of smart card applications to and from the EEPROM. This also applies to cards already issued. This process is called dynamic loading and deleting. The application loader, the loading procedures and data formats are part of the MULTOS specifications.

Recently we have seen many companies teaming up to provide smart card users with extra benefits. Creators of the web's currency beenz.com and Mondex International have teamed up to work on the development of a Multos smart card capable of carrying Mondex e-cash, beenz and complimentary e-commerce services. These companies envision that the card will be used with PCs, wireless devices and digital TV. Mondex is cash in electronic form and is particularly suited to high-volume, low-value payments in the real and virtual world. Beenz on the other hand is a universal web currency. Beenz cannot be bought directly by consumers but are earned online by consumers visiting, interacting with, or shopping at web sites, and in turn can be spent by consumers on thousands of products with participating merchants. Beenz now have the potential to be earned in the real world as well as on-line in the virtual world.

A leading credit card company (American Express Blue Card) has recently launched the first main stream US credit card with both magnetic strip and smart card chip. The company, as part of its launch, is offering a free "on-line wallet" storing personal information that can be secured with a free smart card reader that connects to the users PC. A PIN "unlocks" the wallet online when the smart card is inserted into the reader. The major benefit of this is that the user does not have to keep typing in their account details every time they wish to purchase online.

The predicted "killer application" for smart cards is the loyalty card. This application is really taking off in the US with companies such as the drug store Rite-Aid and the video rental chain Blockbuster leading the way. The smart card loyalty scheme is transacted at the point of sale (POS) terminal and offers discounts and other incentives dependant on how many loyalty points are earned. Rite-Aid also sells a smart card gift certificate, which is redeemable against merchandise in the store with stored value programmed into the chip.

What is a Smart Card Reader?

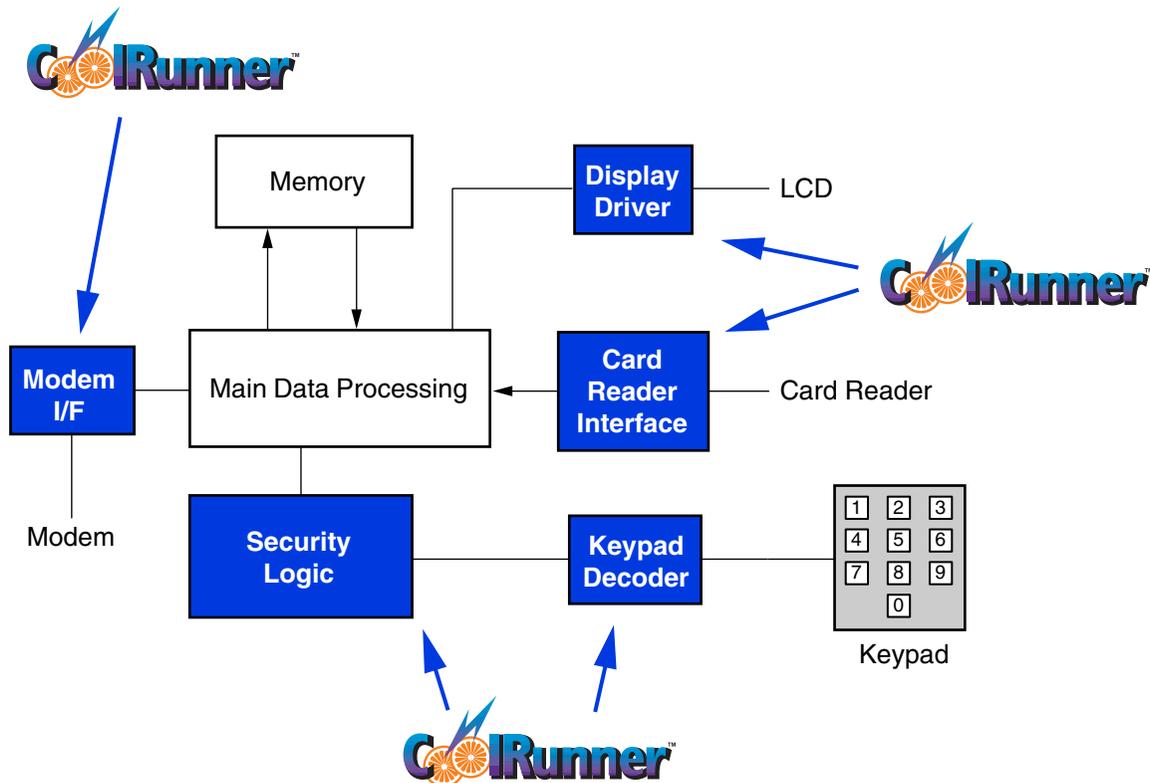
An essential part of the smart card system is the card reader. The card reader is used to exchange or transfer information. There are several types of card readers, each specific to a particular application. They range from a card reader that connects to a PC to enable purchases via the internet (e-commerce) or load money onto a smart card through online banking, to handheld wireless terminals used by taxi drivers and in restaurants.

There are two main categories of smart card reader:

- Contact smart card reader
- Contactless smart card reader

The main difference between them is the contactless version has the addition of an antenna coil to send and receive data without the need to actually make contact with the smart card. The basic functionality of both types of smart card reader is the same and with the introduction of the combicard (both contact and contactless functions on one card) the card reader may have both forms of card interrogation and interaction. The contact smart card tends to be used for cash transactions whereas the contactless type tends to be used more for access control applications.

Figure 3 shows the basic components of a smart card reader for use in retail outlets, taxis, restaurants, etc. Smart card readers for use with PCs would use the PC for inputting data and the monitor for viewing the status of the card. Smart card reader functions may also be integrated into cash registers, vending machines, public payphones, set top boxes, mobile phones, utility meters, etc.



WP118_03_051700

Figure 3: Example of a Smart Card Reader Internal Functions

Xilinx CoolRunner CPLDs are used in hand-held battery powered type smart card readers as they are ideally suited to ultra low-power applications where battery life and size/weight are critical concerns. The CoolRunner range of devices are available in both 3.3V and 5V versions thus enabling smart card reader designs to accommodate both the new 3.3V smart cards and the older 5V types.

The functional blocks that make up the system are:

- Main data processing, this is typically a 16- or 32-bit microprocessor for computational functions
- Memory, to store data (operating system and variable/data storage) and microprocessor boot code
- Security logic to aid data encryption
- Card reader interface, smart card reader (contact and contactless) and magnetic card reader
- Keypad and keypad decoder for entering PINs and other data and the associated logic to decode the characters input
- LCD Display driver
- Modem and modem interface, interfacing to wireless, cellular and radio modems (usually PCMCIA type)

In order to describe the functions of the smart card reader we will walk through a typical consumer transaction. The merchant will insert the smart card into the card reader and power is applied to the card. The reader communicates with the smart card MCU to perform the card authentication cycle. During the initial read function the smart card interface logic will pass the data to the card reader microprocessor via the security logic. The reader will then instruct the user to enter a PIN via a message on the LCD. The user will enter their PIN via the keypad; this will be authenticated by the reader microprocessor. The PIN is verified by the microcontroller in the card which compares with the PIN stored in its RAM with the one presented. If the comparison is negative the CPU will refuse to work. The smart card keeps track of how many wrong PINs are entered and if it is over a predetermined number, lets say three, the card blocks itself against any future use. The amount to be deducted will be entered by the merchant if the PIN is verified and again the smart card will be interrogated to see if it has a stored value to the correct amount, the deduction of the stored values then occurs. If the transaction is not a SVC transaction then the amount to be debited from the bank account will be verified using the modem (wireless, cellular or radio). When the transaction is complete the card is then ejected and removed. The smart card reader is then ready for the next transaction.

The flow of information between an interface device and a smart card occurs via transport protocols in the form of command-response pairs. In most cases the card reader has the role of master, i.e., the commands will be generated and processed by the reader.

Xilinx CoolRunner programmable logic devices can be used to perform the interfacing and decoding functions between the main sections. The main CoolRunner tasks are the memory interfacing and input/output expansion, keypad decoder logic, LCD interfacing, modem interfacing and interfacing to the physical card reader itself. Not only do the CoolRunner devices allow the smart card reader to be updated in the field via in-system programmability (ISP) thus increasing the effective system life but they offer ultra low power operation which is ideal for hand held readers. Hand held smart card readers are becoming smaller and smaller so that they can be used in more varied locations, such as taxis and buses. This drive towards smaller smart card readers necessitates putting the discrete logic (such as standard 7400 series logic devices) into small form factor CPLD devices and this can dramatically reduce PCB area and layers.

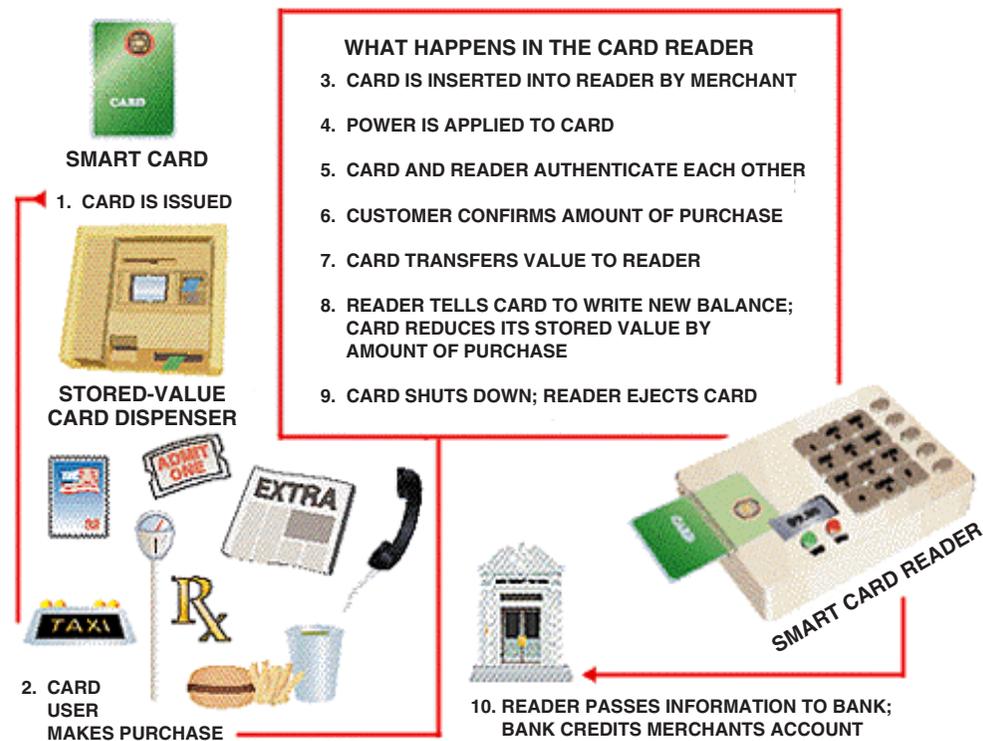


Figure 4: Smart Card Reader Process Flow

Conclusion

Smart cards are making the high technology applications of the twenty-first century easier and more secure for everyone. The smart card market is on the brink of realizing its full worldwide potential, not just in GSM phones but on a wider scale for cash-less transactions, loyalty schemes, access control systems, medical record cards, etc. This year we will see personal computers shipped with smart card readers as standard equipment which will unlock widespread worldwide acceptance of multi-application smartcards. Hand-held battery powered smart card readers in taxis and buses will become common place.

Xilinx high-volume CoolRunner CPLD devices provide smart card reader designers with cost effective solutions that retain the traditional PLD time to market advantage but with the added benefit of ultra low-power operation and very small form factor packages.



Glossary of Terms

ATM	Automatic Teller Machine
CPLD	Complex Programmable Logic Device
DES	Data Encryption Standard
EEPROM	Electrically Erasable Programmable Read Only Memory
FZP	Fast Zero Power
GSM	Global System for Mobile communications
IC	Integrated Circuit
ISO	International Organization for Standardization
LCD	Liquid Crystal Display
MAOSCO	Multi-Application Operating System Company
MCU	Microcontroller
MEL	MULTOS Executable Language
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PLL	Phase Lock Loop
PIN	Personal Identification Number
POS	Point Of Sale (Terminal)
RAM	Random Access Memory
ROM	Read Only Memory
SIM	Subscriber Identification Modules
SVC	Stored Value Card
VM	Virtual Machine

Revision History

The following table shows the revision history for this document.

Date	Version	Revision
05/18/00	1.0	Initial Xilinx release.