Smart Card:
The Computer in Your Wallet

MIPS Technologies, Inc.
June 2002

Smart cards, credit-card-size pieces of plastic incorporating a silicon chip, comprise the highest volume computing platform. Roughly 2 billion are currently in use worldwide and that number is expected to double by 2005. Smart cards are used in everything from cell phones, payment systems, banking and building access, to driving licenses, passports and set-top boxes. Technology is enabling an enormous number of new applications, and the highest market growth is expected to be in 32-bit smart cards. The top five smart card semiconductor vendors have now launched 32-bit smart card ICs that, by 2003, will begin to make a major impact in the capabilities of smart card systems. This article discusses the current status of smart cards within their various market segments and the technology trends that are driving new solutions.

Smart cards are a unique blend of three major technology areas: state-of-the-art silicon memory technology, passive and active security, and microprocessors with high performance but extremely low power consumption. A typical smart card looks like a credit card with a silicon chip. The chip is activated through a characteristic set of contacts or through a radio link. New form factors have started to appear with different shapes and interfaces.

The smart card market can be loosely divided into five segments:

Memory-only smart cards
In memory-only smart cards the chip is a simple memory block with interfaces. These are used primarily for payment systems, such as public telephones and services. While this is currently the highest volume segment, the average prices are lowest, and the market growth is low. Total production in 2001 was 1.25 billion units, rising to 1.7 billion units by 2005.

The other four market segments are technologically more interesting because the card contains a processor as well as memory, interfaces and security blocks. Taken together, these segments will show growth from around 700 million units in 2001 to over 2 billion units in 2005. They consist of SIM (phone), financial, government, and other uses. Though they are well-defined today, their boundaries will merge and change over time with the advent of multi-function cards.

SIM cards
SIM cards are a well-known component of most cellular phones, and their inclusion in next-generation specifications has guaranteed this will continue. The smart card is the part of the phone that is owned/controlled by the operator, rather than the handset manufacturer, so this is where the key to value-added services will reside.

2001 was a poor year for handset sales, so estimates of SIM shipments are around 320 million units. This is estimated to increase to 550 million units by 2005, depending on the world economic recovery, and uptake of third-generation services. SIM cards have various functions, the most important being to provide secure network access to authorized users, and to allow service personalization and a superior user experience.

The hardware that has evolved to meet these requirements comprises a $10mm^2$ chip based on 0.35-micron technology, with 32K or 64K bytes of EEPROM, and 1-3K of RAM. The processor is generally 8-bit, either 80C51- or 6502-based. In addition to the processor, there are other hardware blocks to perform security functions.

The software generally consists of proprietary operating systems designed for small size, with applications such as SIM toolkit adapted for each platform.

The market drivers for SIM cards are coming from both ends of the supply chain. Operators are demanding the ability to provide more services, particularly value-added and transaction-based. For card manufacturers, the drivers are cost reduction and performance. For the smart card OEMs, costs are trending toward development costs rather than IC costs. Future trends include differentiation through software, based on platform standardization with increased processing flexibility. Encryption and security offered in software extends the life of the smart cards as updated algorithms can be downloaded. This flexibility offsets the increased price, validates that each card’s operational life can be extended, and maintains or perhaps decreases the per-year amortization required by the smart card issuers.

One standard that is being introduced is the Javacard operating system. This is a version of Java that can run on an 8-bit processor. Javacard starts to solve one of the problems facing operators, the need to upgrade the services offered, independent of the brand of handset or smart card. The services offered will still be under the control of the phone service provider. With the performance offered by 32-bit MPUs, suppliers have the option to include a hardware Java solution or work with a software Java solution.

Financial smart cards

The banking industry has used plastic cards for identification purposes for many years. But the traditional magnetic stripe has proved very easy to duplicate and copy, so security concerns are driving a change to smart card technology. This market segment shipped around 150 million processor smart cards in 2001, a figure which is set to rise to 430 million in 2005.

Banking smart cards also employ 8-bit processors, along with EEPROM, ROM and RAM memories. Additionally, they usually incorporate a block of logic that assists with cryptographic functions. This is required because, to prevent message interception and decoding, the specifications for handshaking are very tight. The 8-bit microcontroller is not capable of running the cryptography algorithm fast enough to comply with this time limit by itself.

The operating system on a banking smart card has traditionally been proprietary, but recently a secure standard operating system (Multos) has become popular. This is the first operating system to pass all the standards for operational security. On top of the operating system are a series of applications that provide the complex handshaking associated with signature and secure certificate authentication.

The primary market driver for banking cards is increased security. Security is an end-to-end issue for secure systems, of which three parts are relevant to the smart card. These are the ability to encrypt and decrypt data crossing the card interface, the ability to hold the data stored on the card in a secure manner, and the ability to process the data without tampering or breaches in security. This market driver is most dominant in the Asian, South American and East European markets. (The subject of security is dealt with in detail in another section.) The second driver is to value-added services. When a user has multiple credit cards, there is a strong incentive for each issuer to make its card more attractive to use. This driver is dominant in the United States and Western European markets. We can expect to see cards that offer multiple functions provided by the issuer, such as electronic purse, credit card and loyalty schemes.

A new standard is also driving the replacement of credit cards. EMV (Europay, Mastercard and VISA) is a banking standard that allows interoperability of software while preserving high levels of security. By 2005, all credit cards in Europe will use this standard, which will virtually eliminate credit card fraud. It expected that the United States will follow suit by 2008.

Government

Smart cards are used by governments and other authorities to give people access to a variety of services. Smart cards are appearing as passports and driving licenses, and to give access to health and other state services. The key requirements for such smart cards are lifetime costs. Government cards are expected to be in service for many years, so there has to be a facility to add applications to the card in a secure manner. The other key requirement is the storage of large amounts of data. The data includes pictures, such as the photograph of the user, and biometric data such as finger or retinal prints. This information can be used by officials in a spot-check situation to ensure that the bearer of the card is the owner. It will also be possible to add other data such as medical records for use by emergency services.

The process of fingerprint identification compares the result from a sensor to a previous result stored on the smart card. Of course, the stored copy is kept in encrypted form to prevent it from being duplicated or manipulated. The comparison is a complex mathematical calculation that gives the probability of a match, and it could be subject to tampering, either to retrieve the stored data, or to give a false match. Therefore, the most secure place to perform the comparison is on the smart card itself, due to the security implemented on the card. This is driving much higher general-purpose processing performance than is currently available.

Government smart card schemes are in their infancy, so it is hard to give a status of a typical hardware configuration. However, a good example is the E-cities project in Japan. Its aim is to give the cardholder access to a number of services, from transport to information and health. It can also include permits. A 1-million unit pilot program has just been undertaken using smart cards with up to 1 Mbyte of storage, which allows photographs and fingerprints to be securely stored on the card. When the project is extended, 32-bit processors will likely be included on the card to facilitate secure processing of this data.

Because government schemes are in their infancy, it is difficult to predict how this market will grow. A consensus estimate is a growth from 13 million units in 2001 to around 350 million in 2005. Consider the schemes that have been announced: In addition to the Japanese project, the Hong Kong government has announced an ID card system which will be deployed over the next 2-3 years. If successful, it will be extended into the People's Republic of China. The rest of Asia is also likely to adopt smart-card-based identification, ahead of Europe and the United States. Therefore, in 2005 the geographic split of the 350 million units sold may be 30% in China, 20%

in the rest of Asia, 15% each for Europe, Japan and the United States, and 5% for the rest of the world. However, the increased awareness of security issues may accelerate the process of tamper-resistant identification into the United States, which could create a large upside to this projection.

Other types of smart cards

There are many other uses for smart cards. Segments that are large enough to be counted include loyalty cards, building access, pay TV, PC login and multimedia, transport, and experimental.

The loyalty card market was 38 million units in 2001, and will rise to around 60 million in 2005. This slow rate of growth is due to the addition of loyalty applications to other smart cards such as SIM and banking cards. Approximately 60 million building access smart cards were shipped in 2001. These usually employ contactless technology, where the card is powered and communicates using a radio frequency signal.

Smart card technology is becoming an integral part of pay-TV services. Applications are downloaded to the card, which allow it to provide decryption keys to the set-top box for encoded video channels. Around 50 million units were shipped in 2001. This figure will rise to around 100 million units in 2005. Today, the decryption key is provided by the card, but the streaming decode is performed by another IC in the set-top box. This creates a potential security hole between the card and the reader. The best solution is to perform the decode function on the card, in its uniquely secure environment. However, a bottleneck exists in the interface between the card and the reader, so either the interface must change or the secure environment must be moved from the card to another location within the box. Different manufacturers are exploring both of these options. Although the form factor may change, the concept of a trusted and secure IC remains.

In transportation, there are increasing numbers of systems using smart card technology to provide flexible access that depends on the fare a user pays.

32-bit smart cards

It is apparent from this brief market analysis that there is significant development in smart card requirements. The main drivers are security, the ability to run advanced operating systems, addressing larger memories, and the need for more general-purpose processing.

The solution is to migrate to a 32-bit RISC microprocessor within the smart card. This assists in solving most of the problems, with some unexpected additional benefits.

32-bit RISC processors have a long track record of delivering much higher performance than 8-bit microcontrollers at the same clock frequency. For instance, it can take around 20 times more clock cycles to perform a task on an 80c51 processor than a MIPS32™-based 32-bit RISC device. This extra efficiency can be turned into lower power consumption, by reducing the clock frequency, or to achieve extra functionality. An example could be to insert additional instructions in the software to confuse hackers.

Because a 32-bit processor has high performance, the security processing, which once required additional hardware or a coprocessor, can now be migrated to software and performed in the main controller. This not only saves silicon area, but also gives complete flexibility on the algorithms used. No longer are these hardwired into the device during manufacture.

One of the unexpected benefits of 32-bit processors is memory use. By using code compression such as ARM's Thumb or the equivalent MIPS16e™ instructions, code size can be reduced by 50%, compared to 8051-compiled code. This either saves memory or allows much larger programs to be stored.

The top five smart card semiconductor vendors have now launched 32-bit smart card ICs. By 2003 these will be deployed in volume and will begin to make a major impact on the capabilities of smart card systems.

Within the next 3-4 years, a revolution in memory technology is expected. Smart card suppliers are already looking toward new non-volatile memory technology to massively increase the amount of memory available on smart cards. Strong candidates for this technology include next-generation flash, FeRAM, MRAM, etc. Regardless of which one is successful, the performance of the 32-bit processor will be more easily exploited when the program size is less restricted. These memory technologies are likely to be exploited on 0.10-micron process technology. This will also lower the power supply requirements, allowing clock speeds to be increased.

Future applications

It is worth looking a little further into the future and mentioning some additional features on the horizon. The first is the addition of a unique IP address to each smart card. This makes it a unique node on the Internet. The advantage is that the device is then transformed from being a slave to its host (the reader) to being in control of its own communications. Smart cards will initiate conversations and proactively seek data. This will require a protocol stack to run on the card.

Another possibility is the deployment of smart cards with user interfaces. Inputs and outputs such as a keypad and screen can be provided on the device, a capability would drive even more applications in future.

Clearly, smart cards represent an exciting area of technology, offering large volumes with high unit growth. Technology will enable an enormous number of new applications, which will be delivered by end-to-end service providers. Within this market, 32-bit smart cards will offer the highest growth. There will be a trend toward standard processor designs, followed by standard operating systems and, eventually, software. MIPS Technologies has worked with key players in the smart card industry to produce a microprocessor design that has standard instructions, yet also has the scope for complete redesign of security features. This has been adopted by several of the most influential suppliers of smart cards. It meets all the security and processing requirements of the second generation of 32-bit smart cards, while also providing a useful platform for other security devices.

Sidebar

Smart Card Security

There has been a lot of discussion recently about “trusted devices.” Can you trust a PDA or handset with secure data, to make secure transactions, and receive timely and correct information? In fact, most of the capability for trustworthiness resides not in the handset, but in the smart card inside it.

The key reason for having a smart card is for the security of the resident data. So, from a consumer’s perspective, security is considered to be the safety of the data, the ability of the card to resist losing the data, and its ability to securely transfer that data to facilitate transactions.

For the technologist, this translates into three main issues: cryptography and the passing of secure tokens, the security of data, and the tamper-resistant processing of data.

Cryptography

Cryptography is at the heart of the process for passing secure tokens, certificates and data across a network or link. There are two types of cryptographic algorithms: public key and private key.

Private key cryptography enables secure data transfer using previously determined codes between two nodes that are known to each other. An example is a cell phone talking to a service provider to gain a network connection. Messages are free from eavesdroppers and unauthorized users cannot gain access. Commonly used algorithms include Digital Encryption Standard (DES), 3-DES and the new Advanced Encryption Standard (AES).

Public key encryption allows any two network terminals to pass secure messages. The coding uses a composite cryptography key, part of which is public and is sent across the network. The other part is private and is only known to one of the nodes. This allows transactions to be secured against eavesdroppers. Commonly used algorithms include RSA and Elliptic Curve Cryptography.

The smart card has to perform the mathematical functions that constitute these cryptography algorithms. Since the link between the smart card and the reader (such as an ATM) could be insecure, all of the data leaving the card must be encrypted. But timing and power consumption constrain the mechanisms of encryption. The typical approach has been to put a dedicated hardware block on the smart card chip. This is adequate for single-function chips, in which the type of cryptography algorithm is stable for the expected life of the card and known in advance of manufacture. However, for evolving markets and multi-application cards, a better solution is to increase the performance of the processor and enable cryptography in software. This offers lifetime flexibility and lower hardware cost.

Data security

The second area of concern is the safety of the data stored on the card. An attacker will try to remove data for fraudulent use or tamper with it. And attacks can be either physical or electrical in nature. These are prevented by encrypting the data and by making the device in such a way that an attack will, at the very least, delete the data. Most smart cards will also trigger an alert that an attack has been attempted. An attack in which the on-card processor is manipulated to reveal data can be prevented with a rigorous protocol that checks the authority of the request for information. This becomes an issue for the entire security system, not just the card.

Tamper-resistant processing

A third method of attack is to understand how the processor works, then deduce the card's content or security. Two methods are power analysis and fault analysis. Power analysis works by feeding large amounts of 'normal' data into the card, then looking for the power consumption and timing of the processing. In an unsecured system it is possible to feed it a huge number of security keys to calculate the card's security keys. This type of attack can be prevented by injecting random activity into the software so that analysis cannot be repeated. In addition, power smoothing techniques are used to minimize the signals.

Fault analysis attempts to induce errors in the programming by putting abnormal signals onto the smart card contacts. This is often in the form of "glitching" the power supply. When this happens, secure systems with sensitive detectors can shut down the card's operation.