SMART CARDS PROVIDE VERY HIGH SECURITY AND FLEXIBILITY IN SUBSCRIBERS MANAGEMENT

Patrice Peyret, Gilles Lisimaque, T. Y. Chua
Gemplus Card International Corp.
Rockville, MD

ABSTRACT

In conventional Pay-TV systems, the user's decoding key resides inside the decoder box. When pirates crack the code, the security of the system can only be restored by replacing each subscriber's Decoder -a prohibitively expensive solution-. In addition, the Decoder's initial design permanently determines system features -e.g.: number of "tiers"- which can only be altered by a similar system-wide replacement of Decoders.

In **Smart Card***-based Pay Television, the security secrets reside solely in inexpensive and easily replaceable plastic cards -the same size as a credit card, with a secure computer microchip-.*
The Decoder no longer holds any secrets. Replacement Smart Cards can be sent to each subscriber either periodically (e.g., every three months) or whenever there is reason to believe that system security has been breached. With each batch of new cards, algorithms or secret keys can be changed. Attacks on security are therefore extremely difficult to organize, and are not economically viable.

1 ABOUT THE ARCHITECTURE OF PAY-TV SYSTEMS

Pay-TV systems already in existence throughout the world operate in various environments such as cable, terrestrial or satellite transmission media, in NTSC, PAL, SECAM or MAC formats. Most systems may, for convenience, be divided into two parts:

The scrambling/descrambling system

This is the part which processes the program signal (i.e., the video and audio signals) so that the received picture cannot be watched by unauthorized viewers. This physical transformation of the signals is steered in real-time by some logical sequence.
Examples of scrambling systems include such methods as modifying the synchronization part or the active part of the video signal, or altering the sound waveform through digital processing.

The encryption/decryption system

This is the part which "hides" or secures the logical sequence used to drive the de-scrambling process at the receiving end. Encryption usually consists of complex mathematical transformations applied to the data sequence which pilots the physical scrambling sequence.

Examples of encryption/decryption systems include secret polynomiums, secret key or public key algorithms.

The receiving end of the encryption/decryption part, i.e. the decrypting apparatus can usually be further detailed by defining the following two entities:

Access Control Module : control of the access to the program is achieved by making the decryption end of the system operational for only those viewers who have fulfilled certain conditions such as payment. It is the task of the Access Control Module to achieve this by checking the program parameters versus the viewer's entitlements before authorizing any decryption process.

Security Processor : in most cases, the Access Control Module contains a so-called security processor which holds the viewer's entitlements and the relevant secrets in a secure fashion so as to prevent tampering.

Over-The-Air Addressing

When the logical sequence driving the scrambling process is dynamic (i.e., changes in real-time for improved security), it is best to use the same physical channel as the one used for the program signal to send the data flow representing the logical sequence to the audience of viewers.
Systems including this feature are called
In-Channel Addressing
or **Over-The-Air (OTA) Addressing**.

The data flow carried together with the program signal is called the **access-control data**. As an example, NTSC systems can use available lines inside the Vertical Blanking Interval to carry the access-control data while MAC systems can use a part of their data packets.

In OTA systems, the data channel which carries the real-time access-control data is also used to carry two types of information needed for access control:

- individually-addressed customer's entitlements or personal messages
- the current program parameters such as channel identification, date, cost, moral level...

The former information is usually non real-time, and addressed individually or to groups of customers.
The latter is real-time and broadcasted to the entire audience.

Manuscript received June 8, 1990

A block diagram of such a system using OTA addressing is illustrated below in Figure 1 with the encryption and scrambling parts clearly separated:

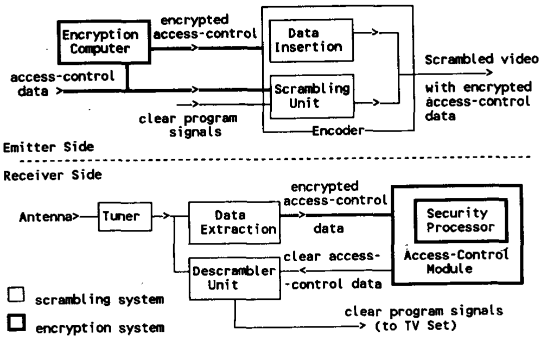


Figure 1

2 SECURITY ISSUES IN PAY-TV APPLICATIONS

The security of any Pay-TV system must be assessed for both the scrambling part and the encryption part. Breaking a system takes the attack of:

- either the scrambling system
- or the encryption system
- or a combination of both

Secure scrambling

Attacking the scrambling part of a Pay-TV system consists of analyzing the physical characteristics of the signal in real-time to find out the scrambling pattern without having to understand the access-control data which drives the scrambling process.

There is a variety of secure scrambling processes to choose from. None of them is totally unbreakable, but some offer a good compromise between security and cost.

RF-level scrambling is very insecure since any person with some knowledge of the frequency characteristics of the perturbation can remove or add the relevant filter to retrieve a clear picture.

Sync-modification scrambling is also very insecure because recent TV receivers with sophisticated sync separation circuitry may very well display an undisturbed picture.

Scrambling based on the modification of the active part of the video signal provides a higher degree of security than the previous two types. Attacking such signals requires auto-correlation or real-time spectrum analysis. Popular methods include Line Cut and Rotate, Video Line Jitter or Video Line shuffling.

The highest level of scrambling security can be found in systems where the signal is processed digitally at the scrambling and descrambling stages of the transmission. This is true for both the scrambling of the video signal and the scrambling of the sound signal. For example, a very strong scrambling system can be built by digitizing the sound signal and shuffling the digitized sound samples in the time domain.

Most often, the scrambling part alone is not the weakest point in a Pay-TV system because attacking it requires sophisticated and expansive signal analÿsis equipment and usually does not yield reliable results in all cases (e.g. when the signal is too uniform, or the picture too dark).

Secure encryption

Encryption/decryption is often implemented as "firmware", i.e. a combination of hardware (such as microprocessors) and software. The software part is the program which represents the mathematical functions needed to operate the encryption transformation.

Because encryption is implemented in firmware, it is often a weak point of Pay-TV systems since this kind of technology is very familiar to the traditional "computer hackers" who are always eager to break into unknown systems.

For example, encryption systems relying on fixed cryptographic functions of which the relevant secrets, such as keys or polynomium coefficients, are always hidden in the same place, are very fragile.

But even more dangerous is the simultaneous attack of both the decryption system and the descrambling system: typically, simple signal analysis of the descrambling part may yield enough information to disclose a part of the decryption sequence. For example, a seemingly robust encryption function such as a polynomial sequence with a large number of coefficients (high degree) can be discovered by accumulating the knowledge of multiple short sequences found out by analyzing favorable signal patterns in the descrambling process.

In most cases, the decryption circuitry sits next to the de-scrambling circuits, which it drives, in the same physical "Decoder" box. Also, when pirates crack the encryption code, the security of the system can be restored only by replacing each subscriber's Decoder - a prohibitively expensive solution -.

The obvious conclusion is that **it is best to remove the decryption part from the Decoder box and fit it in a detachable module.**

3 REMOVING THE SECRETS FROM THE DECODER BOX

By taking all the secrets out of the Decoder box and keeping them in a detachable Security Processor, the system gains the flexibility of being receptive to new algorithms and advances in encryption technology. This is essential since:

- Technology for television security will continue to advance.
- Fixed security algorithms are not secure in the long run (even renown ones such as D.E.S.).

Detachable Security Processor

A detachable Security Processor can be changed if there is reason to believe that security of the system has been breached, or as a preventive means to deter would-be pirates.

It can accommodate more robust encryption algorithms as they are developed, and make use of more powerful microprocessors as they become available at lower costs, thus staying ahead of pirates along the lifetime of the system.

The Decoder box should then contain only the less breakable parts, such as the descrambling circuitry.

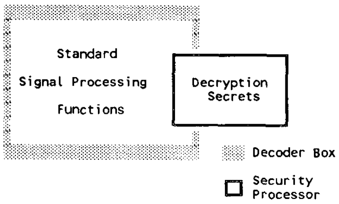


Figure 2

Detachable Access Control Module

As seen in Chapter 1 above, the Security Processor is contained itself in an Access Control Module.

Beside executing the decryption algorithms, the Access Control Module is in charge of interpreting the program parameters (such as date, cost, moral level . . .) and storing the viewer's entitlements. Therefore, its implementation reflects the organization of the Pay-TV operation, i.e. the handling of the subscription services and the customers management methods.

Attempting to define once and for all the subscription methods necessary for Pay-TV services is simply not possible. It is thus essential that the design of any system should remain open to any subscription method and that no parameter interpretation should be hardwired in its architecture.

Hence, detaching not only the decryption processor, but the entire Access Control Module from the Decoder, achieves both unparalleled security and flexibility.

Figure 3 below illustrates such an architecture:

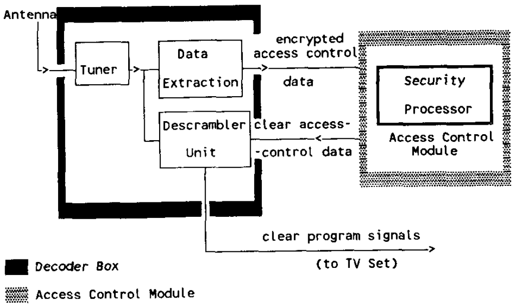


Figure 3

In this way, the Decoder is essentially a descrambling circuit with an interface to the Access Control Module; it is totally transparent to the access-control data.

No pre-determined syntax is required for the access-control data since no interpretation whatsoever needs to be performed in the fixed hardware parts of the system.

4 THE SMART-CARD SOLUTION

A Smart Card is a micro-computer chip including its memory, which is embedded within the thickness of a plastic card the same size as a credit card. All accesses to the memory are controlled by the Central Processing Unit (CPU) contained in the microchip.

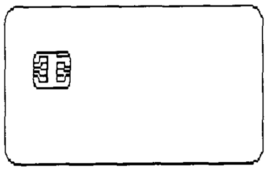


Figure 4

Smart Cards should not be confused with Memory Cards, which are pure storage devices intended to be used in laptop computers, are thicker than credit cards and include multiple memory chips.

The microcomputer chip embedded within a Smart Card is not an off-the-shelf circuit, but a custom-designed device incorporating a range of hardware and software protection and security features. Its interface to the external world is solely through a serial asynchronous electrical bus.

The dimensions, mechanical characteristics, and electrical interface of Smart Cards have all been specified by the International Organization for Standardization (ISO).

Thanks to its local processing capability, storage capacity, and security features, the Smart Card is a perfect candidate for the implementation of a detachable Access Control Module.

Smart Card - based Decoder

A Smart Card-based Decoder is indeed a descrambler box fitted with a slot interface, very much similar to the slot of an Automatic Teller Machine.

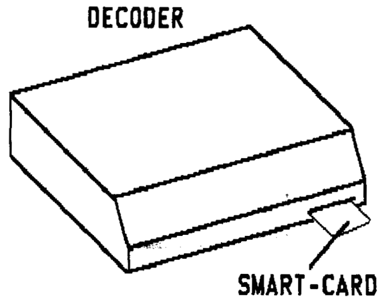


Figure 5

All secrets are stored inside the Smart Card. The Smart Card is an active device which processes the decryption algorithms in real time; as soon as the Card is pulled out of its slot, the Decoder is no longer fed with the data flow necessary to descramble, and cannot produce a clear picture any more.

One may consider such a Decoder as a transparent reader/writer of Smart Cards which happens to have audio and video descrambling circuitry on board. It is thus quite similar to traditional on-line Smart Card terminals found in other applications such as banking, although its on-line link is only one way: from host to terminal.

Smart Card Architecture

The microchip of a Smart Card has basically the same architecture as any micro-controller chip. The CPU has access to:
* Read Only Memory (ROM), where the fixed program can be held,
* Random Access Memory (RAM), used as a scratch-pad for computations,
* Programmable Read Only Memory (PROM) or Electrically Erasable Programmable Read-Only Memory (EEPROM) for storing non-volatile application data or even executable code.

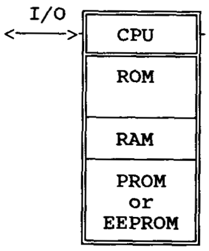


Figure 6

This memory cannot be accessed directly from outside: every access is controlled by the CPU, via a serial I/O link.

The CPU is usually an 8-bit or 16-bit processor core with special protection circuitry such as low-voltage detection, low-frequency detection, light-detection or other proprietary security features.

How to fit a Pay-TV application inside a Smart Card

Developing a Smart Card dedicated to Pay Television consists of writing a specific piece of program which will:

- store securely the viewer's entitlements.
- compare in real time the program parameters such as date, level or cost, versus the viewer's entitlements.
- if the program matches the entitlements, execute the decryption algorithm(s).

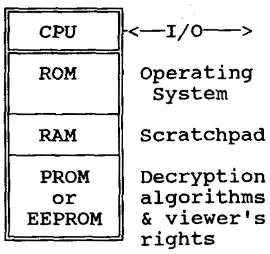


Figure 7

Most Smart Cards come with an Operating System in their masked ROM, which handles all the basic housekeeping functions such as memory management, input/output of characters, and security functions.

The application memory is loaded via the Operating System with the specific executable program (checking of viewing rights and algorithms). With this architecture, the application memory remains under the control of the TV Operator, which can program it in its own way, independently from the Smart Card manufacturer. This process is called **Initialization**.

Conversely, when quantities are large and the system is stable enough, it may be interesting to store the Pay-TV-specific program inside the ROM memory of the Smart Cards in order to leave more space for the storage of entitlements in the writable memory.

Smart Cards can be further **personalized** to hold individual customers' data such as individual viewing rights, name and address, pre-programmed moral level, etc.

Managing Smart Cards Over-The-Air

Smart Cards always have a non-erasable unique ID number. This number can conveniently be used to address individual customers via the Over-The-Air channel. The Card ID is then used as the logical address of the viewer in the system. Therefore, there is no need to personalize the Decoder themselves, and it is not necessary to link a given Decoder to a particular customer.

The Over-The-Air channel can also be used to download new entitlements into each Smart Card. Techniques of group addressing can be introduced to address several Cards simultaneously, when shared entitlements need to be sent to a large audience.

For erasable (EEPROM) Smart Cards, it is even possible to download new executable program such as replacement algorithms Over The Air.

The main Card management function achieved Over The Air is **black-listing** of Cards, i.e. disabling of Cards for those customers who have failed to pay, or for Cards reported as lost or damaged.

5 SMART CARD SECURITY AND ALGORITHMS

Hardware security

Unlike conventional microcomputer chips, Smart Card chips have been designed specifically for security purposes. Their architecture is optimized for security: Smart Card use single chips rather than multiple chips, and have only one serial signal connection to the outside world.

They include a range of protection mechanisms at the silicon level itself:

- the memory patterns of addressing lines inside the chip can be "scrambled" rather than regular, in order to make it more difficult for observers to find out the physical location of any given data.
- a number of silicon sensors are embedded into the chip to detect abnormal conditions such as high temperature, low voltage, low clock frequency, presence of light, etc...
- fuse logic can be used to cut some critical access lines in an irreversible manner.

Passive Card Security through Secret Codes

Memory areas inside a Smart Card may be viewed as small virtual safety vaults, each with its own access Secret Code. The microprocessor of the Smart Card will not grant access to a particular part of the memory unless the relevant Secret Code has been **"presented"** correctly. Furthermore, the Smart Card microprocessor can maintain a count of how many wrong presentations of a Secret Code have been attempted, and take the decision locally to disable definitely the access to an area (or to the entire Card), once a given limit, such as three or four attempts, has been reached. This is called **"ratification"**. Secret Codes can be 64-bit or even longer; several ones can be combined to protect very sensitive areas.

Typically, presentation of Secret Codes can be used during the administrative phases of the life of a Card, to open-up memory areas, create new service entities, etc...

One particular application of Secret Codes is used for Personal Identification Numbers -**"PIN"**-, i.e. a number which the Card's holder must present to the Card for unlocking some functions.

In particular, a PIN code may be used to unlock a Pay-TV Card for the moral level: the Card will allow viewing up until a given moral level, above which it will require the correct presentation of the PIN code (e.g. by an adult).

Active Card Security through cryptography

When a Smart Card is inserted inside a Decoder, it is addressed via its unique ID number by the central Management System with Over-The-Air messages. It is important that those messages cannot be modified before they reach the Smart Card, and in some cases, when privacy must be guaranteed, it may be necessary to hide their contents.

Protection of the integrity of messages sent to the Card can be achieved by means of **"signatures"**. A cryptographic function based on a secret only known to the destination Card is applied to the contents of the message to be protected, and the output result is appended to the end of the message and sent together with it. The Card can locally recalculate the signature with the appropriate algorithm, and verify that it matches the transmitted signature. A pirate trying to modify the contents of such a message will not be in a position to calculate the signature matching the modified contents.

Concealing the contents of the messages themselves can be done through **encirphement** or **encryption**. A cryptographic function F_S based on a secret S known to the Card is applied to the message. The output of the function is the enciphered or encrypted version of the message. The Smart Card applies the reverse function F_S^{-1} to retrieve the message in clear before further processing.

Pay-TV Smart Cards always include such a decryption function, since the main task of those Cards is to permanently decrypt the real-time access-control data sequence which drives the descrambling process. The same function can thus be conveniently used to decrypt service management messages as well.

Active Card Authentication

Despite the hardware protections, and the active and passive security functions described above, there remains the threat of pirates trying to emulate completely a Smart Card by mimicking the behavior of a genuine Card. This can be in the form of some personal computer-based emulator, or even as physical clones if the pirates have made the huge investment of reverse-engineering Smart Cards and producing fake ones.

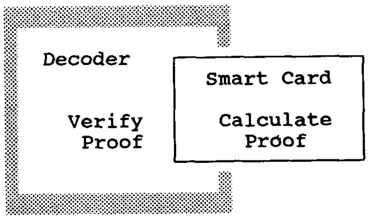
In order to reduce the threat of cloned Cards or Card emulators with diversified ID serial numbers - which would be very difficult to discover -, an authentication scheme is necessary which would force would-be pirates to duplicate false cards with all the same ID number.

In Pay-TV systems, such authentication cannot be based on traditional secret key algorithms since the Decoder boxes, which act as Card readers, cannot know the secret keys stored in the Cards, the system being based on off-line operation.

Thus, it necessary to use a so-called **"zero-knowledge proof"** scheme, i.e. a system whereby the Decoder can determine whether a Card contains a secret it is supposed to have, without the Decoder having to know the secret itself. A well-known example of a zero-knowledge proof system is the Fiat-Shamir algorithm.

Each card's ID number can be "signed" with a function involving some secret code. The zero-knowledge proof algorithm is used to check the authenticity of the card's ID signature without needing to know the secret code.

Obviously, the Decoder must contain the part of the zero-knowledge proof algorithm which is necessary to verify the proof, whereas the Smart Card must contain the part of the algorithm used to compute that proof.



Zero-knowledge proof authentication of the Smart-Card

Figure 8

Pirates attempting to build Card emulators or fake Cards are not able to invent new Card IDs with the proper signature: they are forced to either duplicate a genuine ID, or use IDs with a wrong signature or no signature at all.

The authentication can be triggered at random intervals from the emitting center through the Over-The-Air data channel. Cards with incorrect ID signatures are automatically disabled by the Decoder when the authentication fails.

In order to prevent the message triggering the authentication to be intercepted by pirates, that message should be merged into a larger message containing other essential information, and that larger message should be signed for protection (see above).

This authentication scheme can only be defeated by manufacturing a pirate Decoder without the proof-verifying function. This means that manufacturers of cloned Cards or Card emulators would not be able to sell their system to the installed base of genuine Decoders: they would also have to sell a special decoder.

Card "Fingerprinting"

In case pirates get around the authentication counter-measure by manufacturing fake Cards or emulators with all the same ID number, they can be traced by a method called **"fingerprinting"**.
Fingerprinting consists of including in the Decoder some On-Screen Display (OSD) circuitry which can be used to display the current Card' ID number on the TV screen, super-imposed onto the picture. The command to display the Card's ID through the OSD is sent to the Decoders via the Over-The-Air channel.

With this feature, all the Decoders in the system can be simultaneously ordered to display the ID number of the Card for a few seconds.

Decryption algorithms

The main task of the Pay-TV Smart Cards is to decrypt in real-time the encrypted flow of data representing the logical sequence driving the descrambling mechanism. This is ultimately what all potential attacker of a system will try to discover.

As mentioned above, the philosophy behind Smart Card-based Pay Television is based on the assumption that "fixed" encryption technology is vulnerable to reverse engineering. Therefore, the algorithms execûted by the Cards should be considered as changeable, i.e. be a moving target for potential pirates. By far the most powerful deterrent of piracy is the ability for the TV Operator to change the Cards overnight.

Even better, the TV Operator can change the Smart Cards on a regular basis, therefore changing the algorithms -and any other feature determined by the Smart Card software- even before anyone has come close to breaking into the system.

Each set of Cards can hold two distinct algorithms so that they can be used during overlap periods when a change of algorithm occurs.

Protection against Card theft

When replacement Cards are mailed to customers or stored in retail shops, they are vulnerable to theft.
In order to prevent this, a "chaining" mechanism can be implemented where:

- In order to be operational, a card destined to a given customer must be initialized by chaining to the previous card of the same customer.
- Chaining consists of letting the previous card leave a "message" in a "mail-box" located in the Decoder; that card can then be removed and replaced by the new and yet-unchained card. The new card chains itself through the message left for it in the mail-box.
- An unchained card will refuse to operate on any Decoder. A chained card is operational on all Decoders.

As a summary of the above description of the security features of Smart Card - based Pay-TV, the table below recapitulates the potential attacks and the relevant counter-measures.

ATTACK	ANSWER
Attacking the contents of the Card's memory	Hardware protection
	Presentation of Secret Codes
Attacking the interface to the Smart Card	Message signatures Message encryption
Emulating or cloning of Smart Cards	Active authentication and fingerprinting
Theft of Smart Cards	Chaining mechanism

6 SMART CARDS AS A MARKETING TOOL

Beside bringing in very high security, Smart Cards are also a very powerful marketing tool which TV Operators can take advantage of to offer new services and features.

Flexibility

Because the Encoder and Decoder boxes are transparent to the stream of data used to drive the network, the behavior of the whole system is only determined by the software running in the Subscriber Management Center computers at the head-end and the software in the Smart Cards at the customers end. This means that a TV Operator can actually change its policy about subscription methods, prices, tiering levels, pay-per-view management, by just having new software written, and replacing the Smart Cards.

An Operator is thus no longer dependent on the good will of the manufacturer of Decoder boxes to set up his system and to make it evolve along the time.

Independence

If several TV Operators are to share the same Decoder boxes, - which obviously is the best for the customer - , they do not need to share their secrets and methods of operation. Each one of them can implement his operation in his own way by defining his own Cards with his own commercial logo printed on them. For example Operator "Heaven TV" may want to have only monthly subscription while "K.A.R.D.-News" may implement Pay-per-View: both the Heaven Card and the K.A.R.D. Card will operate in the same Decoder box without the need for Heaven and K.A.R.D. to come to a commercial or technical agreement.

Of course, it is also possible to define multi-Operator cards if needed.

Advertisement support

Cards can be printed just like paper. Commercial advertisements can be put on them and create revenues for their issuers in a way very similar to newspaper or magazine advertising. For example, the french telephone Cards already use this support extensively and cover part of the Cards costs by selling advertisement on them.

Enhancement of TV services

Beside providing new ways of subscribing to TV channels, the Smart Cards can be used to create brand new services. Here are three examples:

Pre-paid Tele-shopping

The cards being a safe electronic fund transfer device, it is possible to store money in them and use them to buy goods advertised on TV. For example, a customer may buy a subscription Card with 50 dollars worth of discounted goods in it (in addition to his usual viewing rights); whenever a product which he wishes to buy is advertised on TV, he can push the "Pay button" of the Decoder box to order the product.

If there is enough money left in the card, the card will record the act of purchasing and decrease the amount of money left accordingly. The customer can then mail his card back or telephone to the sales company to get his product shipped to him.

Interactive games

Because the overall system includes a data channel towards the customers, a means for displaying text on the TV screen (On-Screen Display circuitry of the Decoder), a means for customers to select choices (the remote-control of the Decoder) and a means to store customers' answers securely (the Smart Card), such a system is perfectly suited to implement interactive games.

For example, game Cards can be issued for special sports events such as a football match or a Grand Prix car race. Questions to the audience can be broadcasted in real-time through the data channel of the Pay-TV system, and displayed on the TV screens, inviting people to guess"what will be the score in 15 minutes from now ?" or "How many seconds will pilot X take to cover the next loop ?" The audience will be authorized to answer only during a short period of time, by keying numbers on their remote control units. Their answers are stored in the Smart Card to serve as an unforgeable proof.

Whoever gets the right answer can prove it by mailing his Card back to the TV station or an appropriate center and receive a prize.

The Cards serve both as the authorization to watch the event, and as a game support.

Electronic Coupons

The Smart Card can be used as an electronic rechargeable coupon: during commercials, the viewer can be invited to validate the fact that he is watching the commercial by pressing a button on the remote control or the front panel of the Decoder. This event is securely recorded inside the Smart Card.

After a number of such "commercial-watching" acknowledgements have been recorded, the Card can be brought to a retail store to be used as a coupon, the amount of the discount being a function of what has been recorded in the Card.

Third party support

Viewing cards can be issued also by non-TV Operators on special occasions. Typically, a commercial sponsor can be authorized to distribute special cards through his own retail channels for a specific event.

For example, a manufacturer of soft drinks could have Cards printed with his logo, and distributed through super-markets, which would authorize the viewing of a rock-and-roll concert.

Such Cards can be very low-cost, even without a microprocessor, since the need for security in such cases is much reduced, the Cards being only valid for a few hours or a few days.

7 PUTTING A SMART-CARD PAY-TV SYSTEM TOGETHER

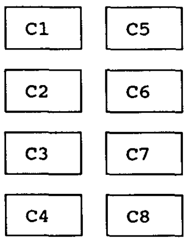
Setting up a Smart Card based Pay-TV system is quite straightforward. It requires that the interface separating the Smart Cards from the rest of the system be clearly defined once and for all, and that the relevant software be written both in the Smart Card, and in a central computer at the emitting site.

Interfacing a Decoder to a Smart Card

As seen above, a Smart Card - based Decoder includes a slot, fitted with a card connector and the appropriate electronic interface circuit.

The physical interface, as well as the low-level communication protocol are described in the ISO international standard IS7816-3. This interface is based on a serial asynchronous protocol operating at relatively low speed - around 9600 bauds -, and using standard TTL-compatible levels for the Input/Output and Clock signals.

A Smart Card interface uses a maximum of 8 physical contacts, the location and the assignment of which are specified in the ISO standard IS7816-2.
The only specific signal is the Programming Voltage which is needed for EPROM-based non erasable Cards. EPROM-based Cards usually require a high-level programming DC voltage comprised between 12 Volts and 25 Volts, whereas EEPROM-based Cards have an on-chip programming voltage generator and only require a single 5 Volt power supply.



C1 = Vcc
C2 = RST
C3 = CLK
C4 = RFU
C5 = GND
C6 = Vpp
C7 = I/O
C8 = RFU

Vcc = Power supply to the Card's circuit
RST = "Reset" signal (from Decoder to Card)
CLK = Clock signal (from Decoder to Card)
GND = 0 Volt reference (electrical ground)
Vpp = Programming voltage (to Card)
I/O = Data signal (bi-directional)
RFU = Reserved for future use

Figure 9

Since most new-generation Smart Cards are now based on CMOS single power-supply EEPROM technology, an interface can be very easily built by using a few I/O lines of a microcontroller port.

Therefore, adding a Smart Card interface to an existing device merely consists of allocating a few Input/Output lines of an existing microcontroller chip to the driving of the Card serial bus.

Writing software inside a Smart Card

Although Smart Card microprocessor chips have special hardware security features, their core is based on standard well-known microprocessor architectures, such as the 6805 or 8048 families. Hence, developing code to be executed by Smart Cards is similar to writing code for any commercial product. The main difference lies in the "debugging" process where the relatively closed architecture of Smart Card microprocessors does not allow the use of off-the-shelf In-Circuit Emulators.
All manufacturers of Smart Card chips offer special emulator boxes to the developers.

As outlined in chapter 4 above, it is possible to use standard generic Smart Cards which have a basic operating system in their ROM memory, and to load the Pay-TV-specific code in the EPROM or EEPROM application memory. This method is very flexible since it allows the Operator to define his system's features - or change them - just before issuing the Cards, independently from the Smart Card manufacturer.

Conversely, the Pay-TV code can be loaded into ROM at the chip manufacturing stage. This frees more application memory and sometimes allows the code to execute faster (because of the shorter access time of Read Only Memory).

Setting up the emitter site

All Pay-TV operations use some sort of Subscriber Management Center where orders, invoices, customers' requests and other management functions are carried out.

In OTA systems, actions generated by the Subscriber Management Center can be addressed to the target customers via the In-Channel data link. Whether a customer is addressable because he owns a decoder box with a unique serial number, or whether he is addressable because he owns a Smart Card with a unique ID number makes no difference to the system. The Subscriber Management System only needs to keep track of which customer has been allocated which Card.

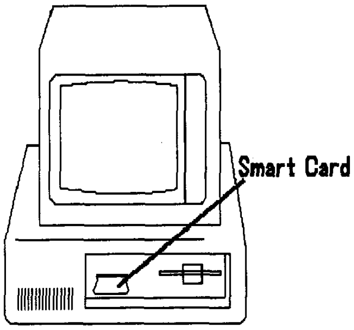


Figure 10

As far as the encryption function is concerned, the emitter site should perform the reverse function of the decryption function stored in the viewers' Cards. This can also be achieved by using a Smart Card programmed to contain the proper encryption function. For example, a computer can be easily fitted with an off-the-shelf Smart Card reader/writer peripheral.

Distribution of Smart Cards

Thanks to its physical dimensions, a Smart Card can easily be mailed in an envelope, or fitted inside a Decoder cardboard package.

Cards can be personalized by printing such things as the Name and Address of the customer onto the plastic. If Cards are distributed through service providers, the logo of the service provider can also be printed. Such personalized printing is carried out by thermal printing machines.

Care must be exercised to not jeopardize the security of the system during the process of distribution. For example, the "chaining" mechanism described in chapter 5 above, can efficiently deter Card theft.

8 CONCLUSION

Introducing Smart Cards in a Pay Television system is a powerful idea which:

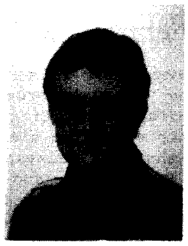
- brings security to unmatched levels
- opens the door to new subscriber management techniques and marketing methods.

Although Smart Cards are still unknown in many countries, the technology is quite mature thanks to the pioneering work done in Western Europe. ISO standards exist, which delineate the low-level functions. New ISO standards are being prepared to cover higher-level inter-industry topics.

Smart Card technology can even be applied to other forms of packaging than plastic cards: some companies have produced keys and other objects, with a smart-card chip embedded in them.

Since Smart Cards are based on conventional silicon technology, they benefit from the tremendous advances achieved in this field. Therefore, using such Cards in a Pay Television system is a future-oriented choice.

Several implementations of Smart Card - based Pay-TV systems have appeared recently or are being announced in the UK, in France, New Zealand, Australia, Germany, Spain, Scandinavia. This is likely to become an essential technology for Pay-TV over the next decade.



Patrice PEYRET

Curriculum Vitae

Position: Product Development Manager
Gemplus Card International

Other responsibilities: Director of Gemplus Technologies Asia (Singapore)

Previous experience:

Held the following positions with Thomson Consumer Electronics:

- 1988–1989: Director of the R&D laboratories in Strasbourg, France
- 1986–1987: Director of the R&D laboratory in Los Angeles, California
- 1982–1986: Head of the micro-computer R&D laboratory in Paris, France