Overview of Card Technologies

A Presentation to
The National Institute of Standards
July 8th 2003

Edward Oppenheimer

Booz | Allen | Hamilton

Introduction

A Quick Look at Today’s Card Technologies

- Magnetic Stripe Card
- Smart Card
- Optical Card
- Proximity Card

What are Magnetic Stripe Cards?

Magnetic stripe cards have a black or brown magnetic stripe made up of magnetic particles or resin.
We use magnetic stripe cards everyday.

Magnetic Stripe Card

Magnetic Stripe Card Common Applications

The cards are commonly used in industries with low-to-medium-data storage needs such as:

- Bank Credit and Debit Cards
- Transit Cards — Subways, Railroads, and Buses, Tolls Roads, Airlines…
- Identification Cards — Driver Licenses, Badges, Employee ID, Membership Cards, Door Keys…

Basics of Magnetic Stripe

- Magnetic Stripe Media
- Magnetic Stripe Equipment
- Magnetic Stripe Tracks
- Data Storage and Retrieval
- Data Robustness
- Magnetic Stripe Capabilities

Magnetic Stripe Media

- The media (cards, badges, and tickets) must be made of non-magnetic material.
- Magnetic stripes must be on the surface of the material in which the stripes are bonded.
- One edge of the media must be straight and parallel to the direction of encoding on the stripe to serve as the locating reference for the read and encode heads.

Data Storage and Retrieval

- The card data is encoded in a binary format, with the polarity of the particles determining the 0-bits and 1-bits.
- A reader detects and decodes the polarity changes, called "flux reversals" and translates the binary code to alphanumeric for processing by a computer.
- A special digital recording (called encoding) of data on a magnetic layer (called a stripe) similar to that on audio and video tape is used, which can then be repeatedly played back (called reading)
- A magnetic stripe can be re-encoded and used over again.

Magnetic Stripe Equipment

Equipment comes in different shapes, sizes, and methods of mechanical operation with two fundamental requirements.

- The magnetic stripe head “transducer” must remain in contact with the magnetic stripe and must remain in motion with respect to the stripe during reading or encoding.
- An encoder must provide for the proper placement of the digital signals, which represent the string of “zero”and “one” data bit encoded on the stripe.

Magnetic Stripe Tracks

Each of the three tracks on the stripe holds specific data:

- Track 1 – An alphanumeric track that holds card holder name, card number, and card expiration date. Its limit is 79 characters.
- Track 2 – numeric only track, contains card number and expiration date, has 40 characters limit, can contain same data as track 1, can be used as a replacement for track 1
- Track 3 – numeric only, is seldom used in the US, can contain 107 characters, usually used when information needs to be read and written back with each use of the card for off-line systems.

Data Robustness

Coercivity is the ability of a property to resist demagnetization. The material used for the particles determines the coercivity of the stripe.

- High coercivity (HiCo) magnetic stripe relies on particles – barium ferrite. HiCo is less susceptible to accidental damage by magnetic fields.

- Low coercivity (LoCo) magnetic stripe relies on particles – iron oxide . LoCo is more susceptible to accidental damage by magnetic fields.

Data Robustness (Cont.)

The easiest way to determine visually if a stripe on a card is HiCo or LoCo is by the color.   Magnetic stripe readers are "blind" as to whether a stripe is HiCo or LoCo and designed to read both.

- HiCo stripes are black
- LoCo stripes are brown

Selecting which Type of Magnetic Stripe

The type of stripe on the card usually determines how the card is to be used.

- HiCo stripe is for applications such as access control cards, time and attendance cards and driver’s licenses where they are to be used frequently (e.g., daily).
- LoCo stripe is for application such as retail customer loyalty cards, membership cards where they to be used less frequently (e.g., once a week or once a month).

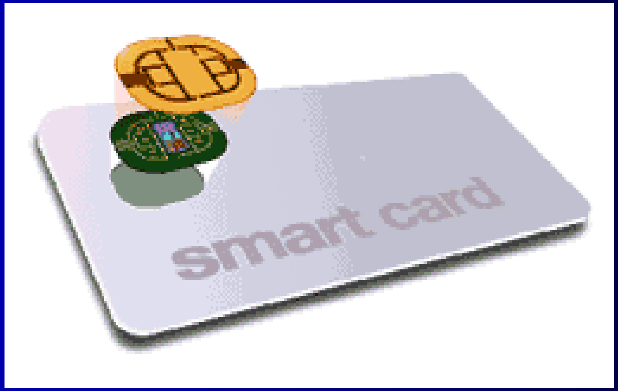
Magnetic Stripe Capabilities

- Values can be added to the card by different means.
- Depending on the card system, magnetic stripe card can provide on-line or off-line access system.
- Reasonably durable materials, particularly for card-based product.
- Different security developments to suite a range of specific application needs.

Smart Card

A smart card is an intelligent credit card sized plastic card embedded with either a microprocessor and a memory chip or only a memory chip with non-programmable logic. Three main types of smart card are:

- Contact Card
- Contactless Card
- Hybrid Card

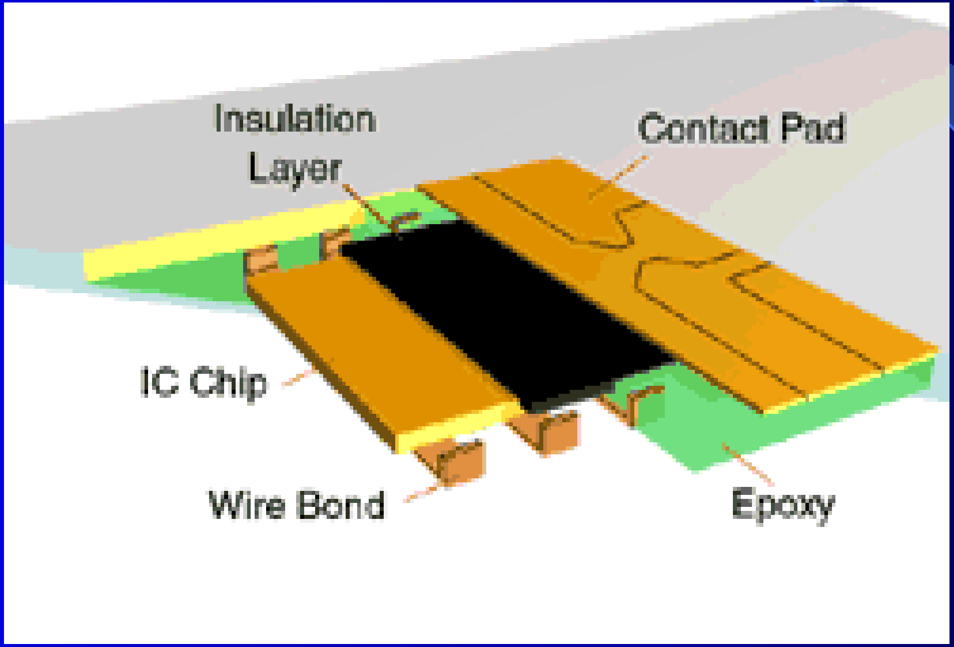


Contact Cards

Contact Cards are frequently used by financial institutions.

- A chip with contact pad (plate) is embedded in the card.
- The card must be inserted into a smart card reader and must have a direct physical contact with the chip's plate to transmit data.

Contact Card Construction



Cutaway View of Contact Card Construction

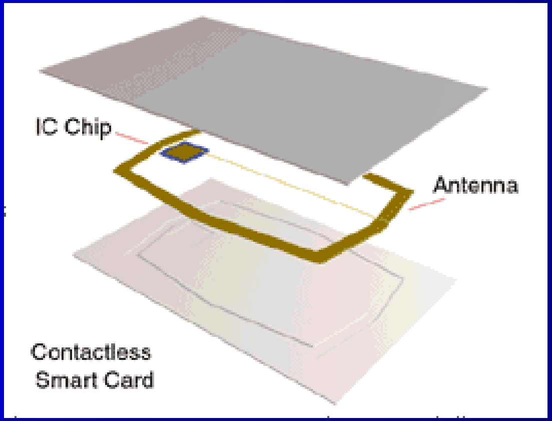
Contactless Cards

Contactless cards are commonly used for access control and transit applications.

- An antenna coil and a chip are embedded in the card.
- The card must pass within varying degrees of proximity to a smart card reader.
- The embedded antenna communicates with a receiving antenna at the transaction point.

Contactless Card Construction

An antenna coil and a chip are embedded in each contactless card.



Hybrid Cards

(also known as Dual-interface cards)

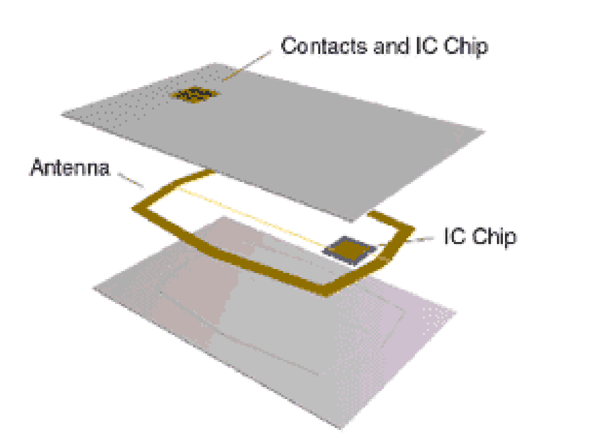
Hybrid cards are commonly used in the mass transit. The contact interface may be used to place a cash toll value on the cards while the contactless interface is used to remove a toll value.

- A hybrid card comes with a contact and contactless chip embedded in it.
- A COMBI card comes with a single chip shared by contact and contactless interface.

Hybrid Card Construction

The two chips (contact and contactless) embedded in the hybrid card may be memory or microprocessor chips. They are not connected to each other.

- Contactless Chip is for applications demanding fast transaction time – like mass transit.
- Contact Chip is use in application requiring higher security.



Basics of Smart Card

- Smart Card Capabilities
- Smart Card Life Cycle
- Smart Card Security

Smart Card Capabilities

Smart cards can carry all necessary functions and information on the card. They do not require access to remote databases at the time of the transaction.

Smart card capability can be described according to two smart card types:

- Memory cards
- Microprocessor cards

Memory Cards

The memory card has no processor on the card to manipulate the data; it depends on the card reader for its data processing needs. Each memory card:

- Communicates through a process that is controlled by the terminal.
- Stores information, access control, or a value that can be used.
- Can hold from 103 to 16,000 bits of data.
- Are less expensive than microprocessor card.
- Offer minimum security, thus they are used in low-to-medium security applications.

Memory Card Types

- Storage-only Memory Cards
- Memory Card with Register

Storage-only Memory Cards

- Have a rewriteable memory
- Are often used in loyalty applications to store a buyer profile. As a buyer spends money, he earns points for which can be redeemed toward various rewards

Memory Cards with Register

- Start with a set of values that decreases with use
- Are not rewriteable; once the values are used up, the cards are discarded
- Are commonly used for prepaid telephone and vending cards

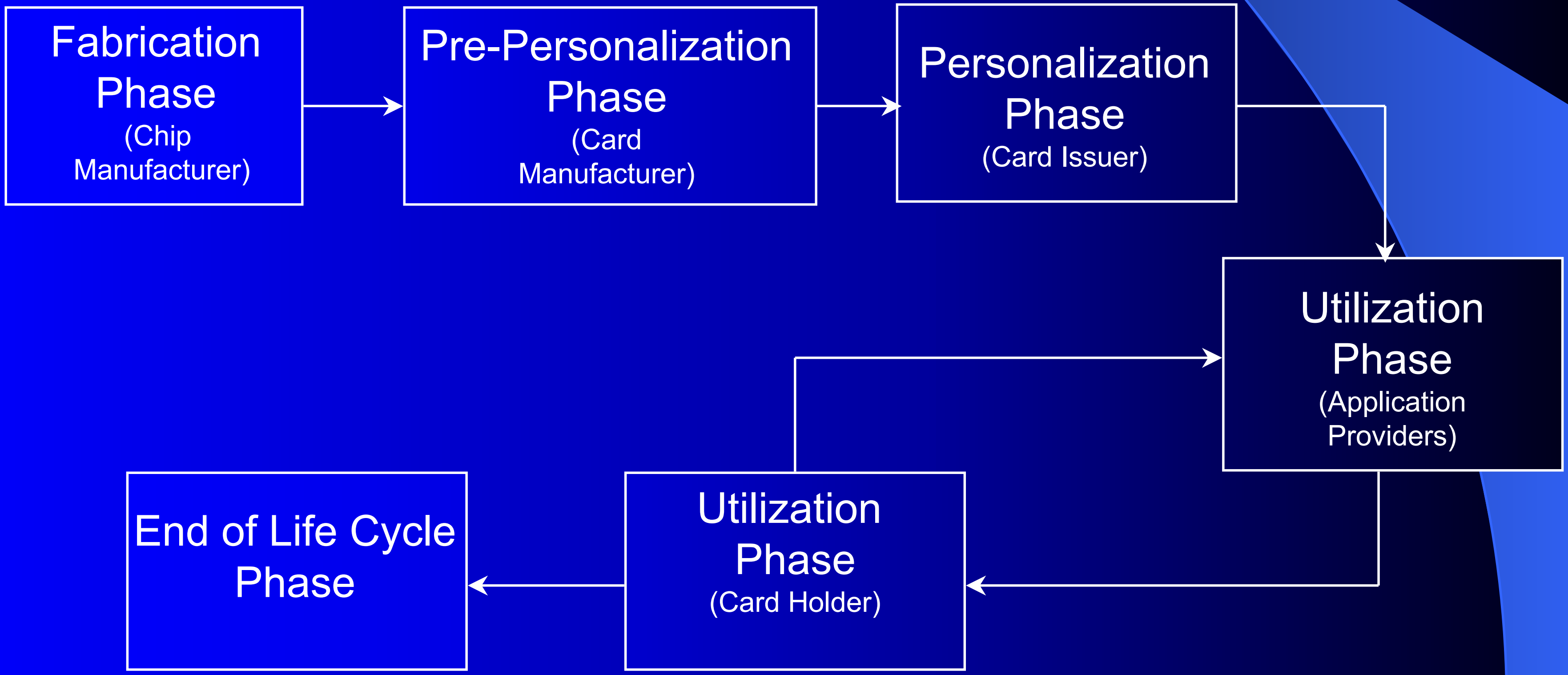
Microprocessor Card

The Microprocessor card has on-board CPU and Operating System that manages access to the data on the card.

- The microprocessor acts as a security gate .
- Self locking mechanisms are invoked if incorrect codes are presented.
- Are commonly used to store electronic money, sensitive data, or security keys.

Life Cycle of a Smart Card

The production of a smart card is divided into different phases from the manufacturer to the application provider, then the card holder. There are five phases for a typical smart card life cycle:



Fabrication Phase (Chip Manufacturer)

Pre-Personalization Phase (Card Manufacturer)

Personalization Phase (Card Issuer)

Utilization Phase (Application Providers)

Utilization Phase (Card Holder)

End of Life Cycle Phase

Fabrication Phase (Phase 1)

This phase is carried out by the chip manufacturer. Here are the steps involved in this phase:

- The silicon integration circuit chip is created and tested.
- A unique fabrication key is added to the chip to protect it from fraudulent modification until it is assembled in the plastic material.
- Other fabrication data is written to the circuit chip at the end of this phase.
- The chip is ready to be delivered to the card manufacturer.

Pre-personalization Phase
(phase 2)

This phase is carried out by the card supplier.

- The chip is mounted on the plastic card which may have the logo of the application provider printed on it.
- The connection between the chip and the printed circuit is made; the whole unit is tested.
- The fabrication key is replaced by a personalization key as an added security to allow secure delivery of the card to the card issuer.
- A personalization lock is written to prevent further modification of the personalization key.
- The physical memory access instructions are disabled. Access to the card can only be done by using logical memory addressing.

Personalization Phase (phase 3)

This phase is conducted by the card issuer; it completes the creation of logical data.

- Data file contents and application data are written to the card.
- Information of the card holder identity, PIN, and unblocking PIN is stored.
- A utilization lock is written to indicate the card is in the utilization phase.

Utilization Phase (phase 4)

This is the phase for normal use of the card by the card holder.

- The application system, logical file access controls, and other are activated by the card holder.
- Access information on the card is limited by the security policies set by the application.
- Multiple applications can be placed on the same card.
- The card holder determines which application provider gets real estate on the card.

End-of-Life Cycle Phase

(phase 5)

There are two methods to move a smart card into this phase:

- The first method is initiated by the application which writes the invalidation lock to an individual file or the master file; all the operations will be disabled by the OS; only read instruction will remain active for analysis purposes.
- The second method is when the control system irreversibly blocks access because both the PIN and unblocking PIN are locked; all the operations will be blocked.

Smart Card Security

Smart card security can be viewed from three different aspects:

- The physical structure of a smart card, and how it protects the data through the card's life cycle
- How the data is protected through the logical controls over the files in the card
- How the smart card can provide a secure and authenticated environments through procedural operation and mechanism

Physical Structure

The physical structure of a smart card is specified by the ISO 7810 and 7816--parts 1 and 2. The structure is made up of three elements:

- A plastic card with the dimension of 85.60 mm X 53.98 mm X .80 mm
- A printed circuit that conforms to ISO 7816/3 which provides five connection points for power and data
- An integrated circuit chip that consists of a ROM, microprocessor, ROM, non-static RAM and electrically EPROM which will retains its state when the power is removed.

Physical Interface

A suite of protocols with the restricted bit rate prevents massive attack on the card. The physical interface:

- Allows data exchange between the integrated circuit chip and the card acceptor device – traditionally limited to 9600 BPS (New USB interface allows much higher interface speed)
- Provides a communication line which is a bi-directional serial transmission line
- Controls data exchange – card commands and input data are sent to the chip which responses with status words and output data upon receipt of these command and data

Logical Controls

After a smart card is issued to a card holder, the protection of the data will be controlled by the application. Access of data has to be done through the access control conditions established by the application provider. Mechanisms and algorithms used to protect data are:

- Logical file structure
- Access Control
- PIN Presentation
- PIN Management

Logical File Structure

The methods used below provide a logical protection of the smart card:

- The use of the root file or master file (MF) which contains elementary files (EFs); under each EF,there are dedicated files.
- Data managed within a file depends on different application providers.
- The logical access and selection mechanisms are activated after the power is supplied to the card while the master file is selected automatically.
- Access of the data in the file depends on whether the conditions is fulfilled or not.
- The attributes of each file is enhanced by adding access conditions and file status fields in the file header. File lock is also provided.

Access Control

The smart card access control system mainly covers file access. The access conditions of a file can be defined into the following five levels:

Always (ALW) - access of the file can be performed without any restriction.

Card holder verification (CHV1) - access can only be possible when valid CHV1 value is presented.

Card holder verification (CHV2) - access can only be possible when valid CHV2 value is presented.

Administrative (ADM) – allocation of these levels and respective requirement for their fulfillment are the responsibility of the appropriate administrative authority.

Never (NEV) – access to the file is not allowed.

PIN Presentation

The PIN on a smart card is normally stored in separate elementary file, EF CHV1 and EF CHV2. The PIN is blocked when a fixed number of invalid PIN are entered consecutively. Unblocking has to be carried out with:

- The correct PIN and a specific unblocking PIN stored in the card.
- The unblocking PIN will also be blocked if entered incorrectly up to a variable number of times.
- When the PIN and unblocking PIN are blocked, it is called irreversible blockage; both PINs will be invalidated and can no longer be restored.

PIN Management

Two counters have to be implemented for each of the card holder verification number (CHVs) in order to achieve the protection and blockage of the PINs. There are three states in the management of PIN:

- PIN has been presented – File functions can be carried out.
- Valid PIN has not been presented – the PIN counter will be decremented by one.
- PIN is blocked – Unblocking PIN instruction has to be carried out. If correct unblocking PIN is present, the PIN counter will be reset to the maximum number of tries and backed to the first state.

Procedural Protection

Procedural protection is divided into three main areas.

- Identification of documents
- Authentication
- Access control on operating system

Identification of Documents

The smart card is probably the best solution for traditional document-based identifications.

- Access condition and password are set up on file; only authorized persons are allowed to access the information.
- Biometric information of the card holder can be placed on the card, so that the smart card can corporate with biometric scanner to identify whether the card is owned by the card holder or not.
- The use of a card receptor is used to verify the information instead of verifying the documents by observation of an inspector officer.

Authentication

(using Kerberos system as an example)

Kerberos is one of the system that provides trusted third-party authentication services to authenticate users on a distributed environment (smart card environment). Kerberos authentication system uses the following feature:

- When a user requests an access to a particular service from the server, he has to obtain a ticket for credential from the Kerberos authentication server (AS). The user then presents that credential to the ticket granting server (TGS) and obtains a service ticket; hence, the user can request for service by submitting the service ticket to the desired server.

Access Control on Operating System

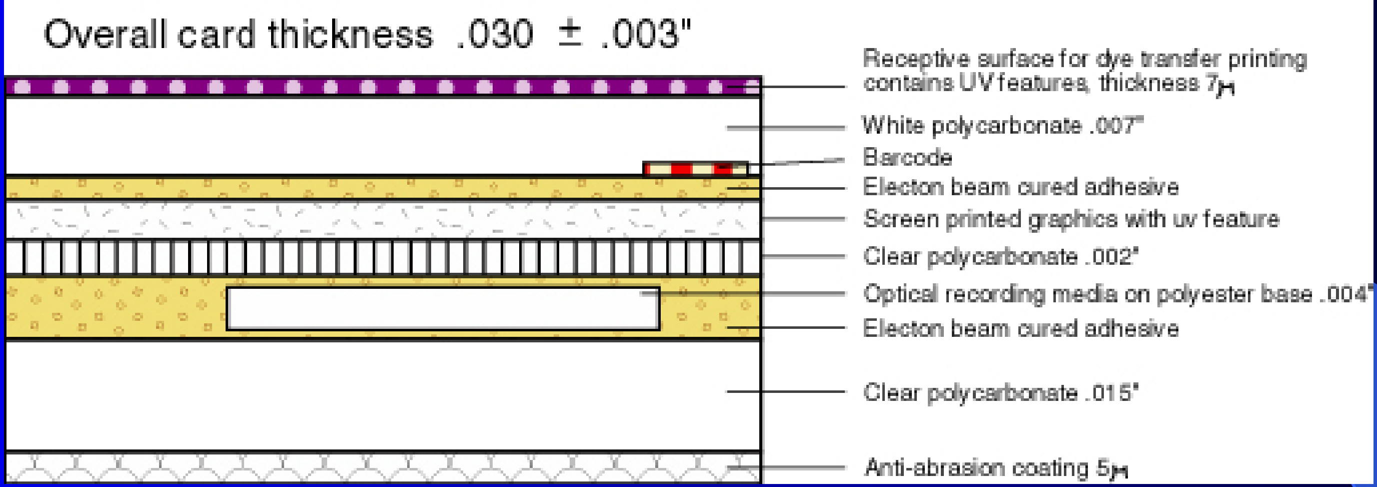
Access control is one of the most important usage of the smart card technology. A boot integrity token system (BITS) is introduced to protect the operation system.

- A host computer is booted actually from a smart card or it requires critical information from the smart card to complete the boot sequence.
- Two authentications have to be performed before the completion of a boot sequence during the system startup.
- A smart card can also store the checksum of critical data and executable programs.

What are Optical Cards?

Optical cards are also called laser cards. They are the same size and shape as standard plastic credit cards. The material is comprised of several layers that react when a laser light is directed at them. The media is write-once-read-many (WORM).

Optical Card Construction



Overall card thickness .030 ± .003"

Receptive surface for dye transfer printing contains UV features, thickness 7μ

White polycarbonate .007"

Barcode

Electon beam cured adhesive

Screen printed graphics with uv feature

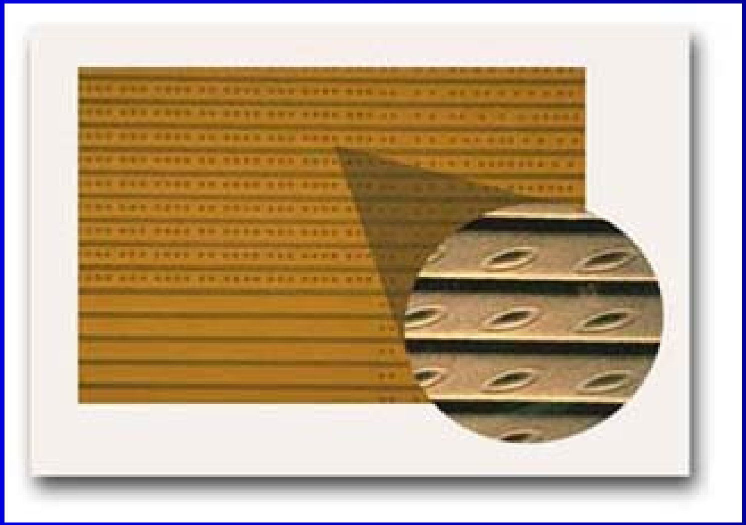
Clear polycarbonate .002"

Optical recording media on polyester base .004"

Electon beam cured adhesive

Clear polycarbonate .015"

Anti-abrasion coating 5μ



Source: www.lasercard.com

What kind of Data is Stored on Optical Cards?

Data that can be stored on optical cards include:

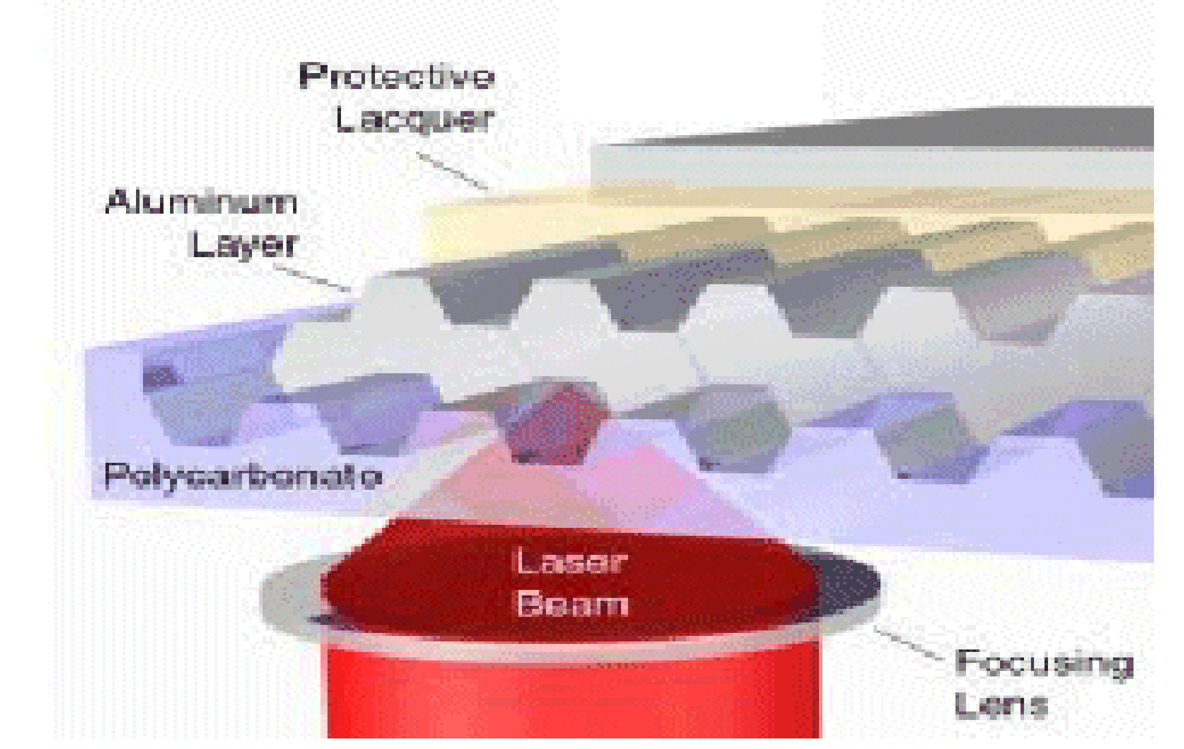
- Cardholder name, address, and other personal information
- Digitized cardholder photographs
- Signature
- Medical images or x-rays
- Updateable account balances and transaction audit trails
- Security information

Optical Card Technology

Optical cards use a technology similar to the one used for music CDs or CD ROMs.

- A panel of the “gold colored”laser sensitive material is laminated in the card and is used to store information.
- The material is comprised of layers that react when a laser light is directed at them. The laser burns a tiny hole in the material, which can then be sensed by a low power laser during the read cycle.
- The presence or absence of the burn spot indicates a “one” or a “zero”.
- The data is non-volatile and is not lost when power is removed.
- Data is encoded in a linear x-y format.
- ISO/IEC standards 11693 and 11694 define standards for optical cards.

Encoding an Optical Card



Optical Card Applications

Optical cards are data intensive cards. Different optical card applications are used worldwide to:

Store - Prenatal-care records

- Medical images and personal medical records
- Auto repair/warranty records

Serve as - High-security driver license

- Access/entry cards
- Secure bank debit cards
- Immigration identification cards

Optical Card Applications (cont.)

Government applications:

- LaserVisa — the US Immigration and Naturalization Service uses them as Permanent Resident and Border Crossing cards.
- Automated Manifest Systems — the US Defense Logistic Agency uses this application to manage its enormous shipping and receiving system.
- LSC VAR Laser Memory Cards — the Italian government uses them as a key security component in an Italian national ID card.

Optical Card Application (Cont.)

Consumer Applications:

- The VisionKey card serves as a single-user ticket for a proprietary laser vision correction and phototherapeutic Keratectomy system. The card stores a patient's record for the procedure: pre-and-post-op patient data, prescription, treatment algorithm, and eventually may include a video transcription of the 30 second procedure.
- The LaserCard gives the Honda car owner in the Philippines a complete vehicle history which they can carry in their wallet.

Optical Card Capabilities

Optical cards can store between 4 to 6.6 MB of data. The card is a special case of distributed data in that a person's records will reside on the card in such a way that they may be retrieved for use in the system.

- Once new records are collected or existing records for the person are revised, they can be written back to the card as well as to the larger database.
- The card can perform off-line card verification.
- Card update can perform 30 times faster than chip-cards.
- Each card has a permanent and very secure fraud-proof operation using the latest crypto technology.
- No possible loss of data from exposure of cards to static electricity, water, magnetic, electrical fields, or x-rays.
- The card allows storage of the biometric template in encrypted form.