# E-Payment Systems and Cryptocurrency Technologies

https://course.ie.cuhk.edu.hk/~ftec4004

Prof. Wing C. Lau
wclau@ie.cuhk.edu.hk
http://www.ie.cuhk.edu.hk/~wclau

# Smartcard Technologies, EMV, RFID, Contactless Payment Cards and Stored Value Facilities (SVF)

# Acknowledgements


- The slides used in this lecture are mostly adapted from the following sources. The copyrights and contribution of the original authors are hereby acknowledged and recognized:
  - The Electronic Payment Systems course by Prof. Michael Shamos, CMU
  - Matt Davies, “Hot Topics in Payments,” Federal Reserve Bank of Dallas, Oct 2014
  - Leanne Phelps, “EMV, Tokenization and Apple Pay: The New Landscape,” Oct 2014.
  - Seth Harrington et al, “What’s NOT in your Wallet ?”, Ropes & Gray, #iLAW Summit, Mar 2015.
  - Richard Martin, “Secure Mobile Payments: getting the balance right, “ Sept 2013.
  - Guido Mangiagalli, “Wave and Pay – Visa Contactless,” Visa Europe, 2005.
  - Smart cards : the developer's toolkit, Tim Jurgensen, Scott B. Guthery, Prentice Hall 2002
  - Smart Card Technology and Applications, Scott B. Guthery, Timothy M. Jurgensen, 2000.
  - Nguroho Gito, “Card Payment: Overview of Evolutions, Technology and Business”, IBM, 2018.
  - Biometric Payment Cards, A Secure Technology Alliance Payment Council White Paper, March 2019.
  - Smart card handbook, 4th Edition, Wolfgang Rankl and Wolfgang Effing ; translated by Kenneth Cox, 2010.

# Smart Cards


- What is a Smart Card** ?
  - A small portable computer, without a display, keyboard or power-source ;
    - Integrate a 8-32 bit 30+ MHz microprocessor, upto 256KB's ROM and 1-8KB RAM, plus some Apps
  - *Often* the size of a credit card (common exception: SIM, micro SIM, nano SIM) ;
  - Use in conjunction with a Contact or Contactless reader
- What is it for: Securely Identify and Authenticate the Cardholder and 3rd parties who want to gain access to the card's info
- PIN-code or Biometric Data can be used for authentication
- Also provide a way to securely store data on card and protect communications with encryption
- Market: 30-50 Billions smartcard in circulation already ; Another 10 Billion expect to have been shipped during 2020.
- Major Players: Gemalto/THALES, Giesecke &Devrient, IDEMIA (formerly Oberthur Technologies and Morpho), NXP, Samsung, STMicroelectronics

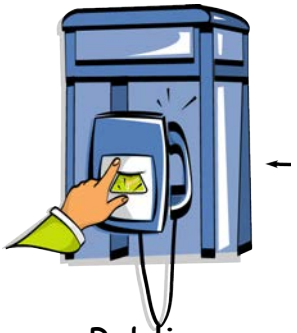
** Sometimes, not-so-smart cards are also broadly referred to as "smartcards" as well, e.g.
Magnetic stripe - 3 tracks, ~140 bytes, cost $0.20-0.75
Memory cards - 1-4 KB memory, no processor, cost $1.00-2.50
Optical memory cards - 4 megabytes read-only (CD-like), $7-12

# Smart Card Applications

E-Government

Banking

Mass Transit



Public Telephony

Mobile Telecommunications

W-LAN


Retail

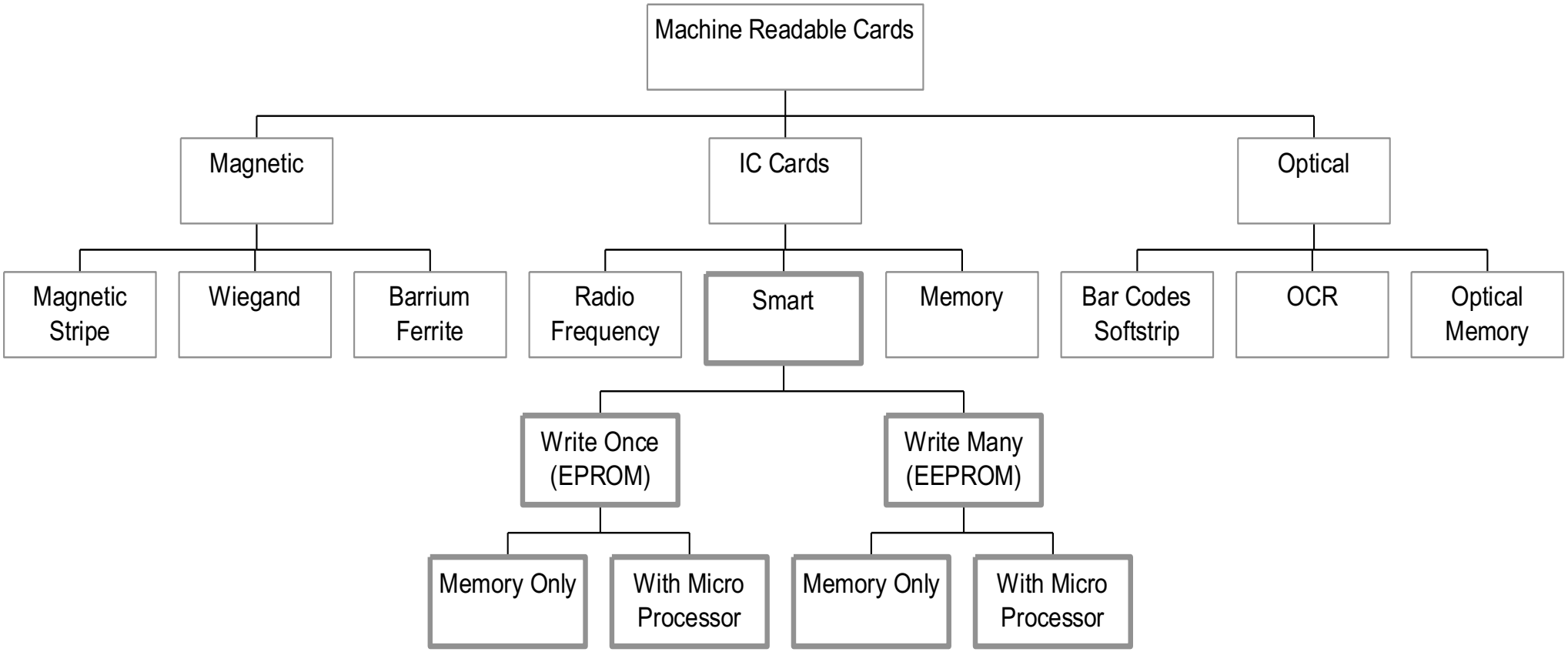
Access control

Enterprise Security

Digital Rights Management

SOURCE: JEAN-JACQUES VANDEWALLE

# Card Taxonomy (circa 2000)




SOURCE: BURGER, CAROLL & ASSOCIATES

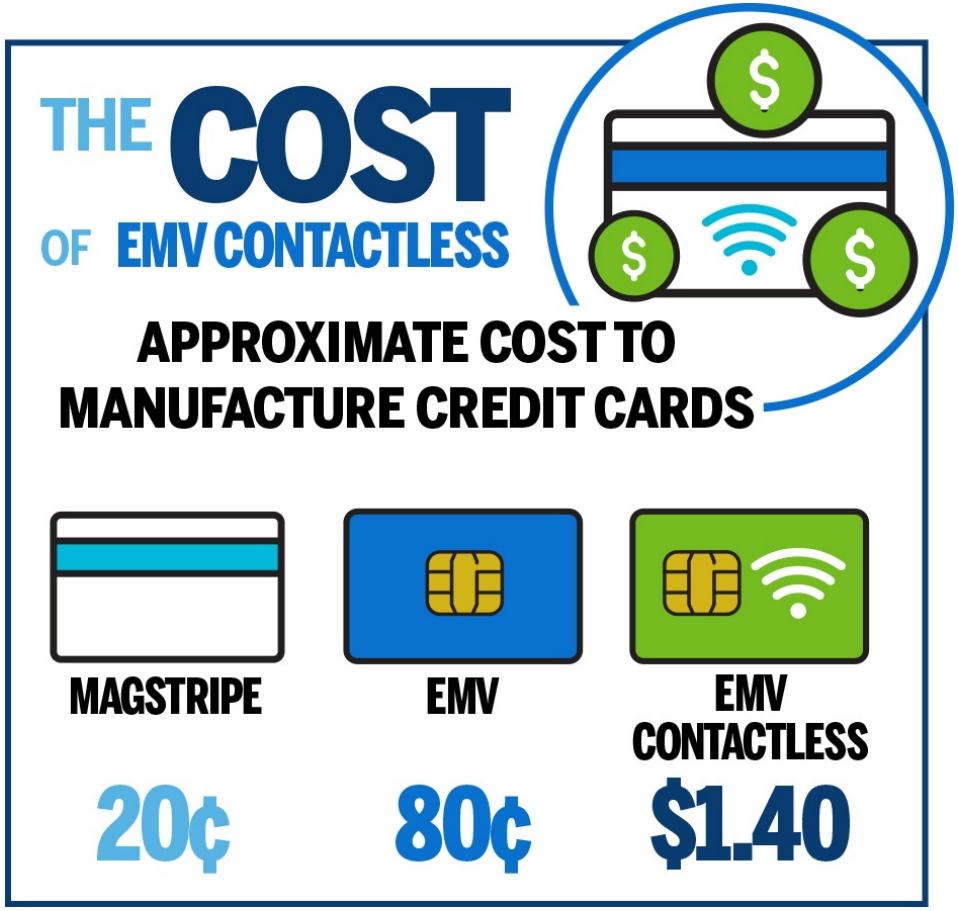
# History of Smartcards

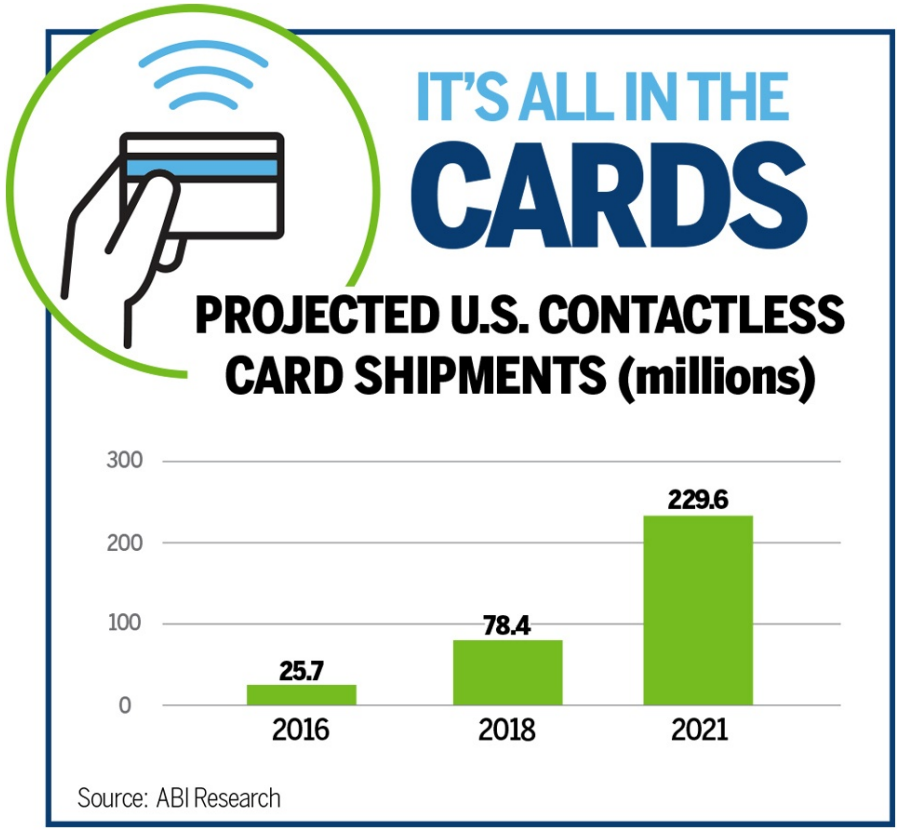
- 1974: Roland Moreno patented the memory card.
- By 1977, three commercial manufacturers Bull CP8, SGS Thomson, and Schlumberger, started developing smart card products.
- In March 1979, Michel Hugon from Bull CP8 was the first to design and develop a microprocessor-based card combining a processor and local memory. He invented the computerized smart card.

1979: early developments for the banking sector
1995: first SIM cards
1999: first national eID card (Finland ID)
1999: first smart cards for transport
2001: The Department of Defense first issued Military CAC credentials for physical access control and secured logical authentication
2003: Micro-SIM launched
2005: first ICAO-compliant electronic passport (Norway passport)
2012: Nano-SIM introduced
2018: first biometric contactless payment card, eSIM launched (thickness is <1 mm or 0.039 in)
2019 First 5G SIM available

SOURCE: https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/smart-cards-basics

# Cost of Smart Cards



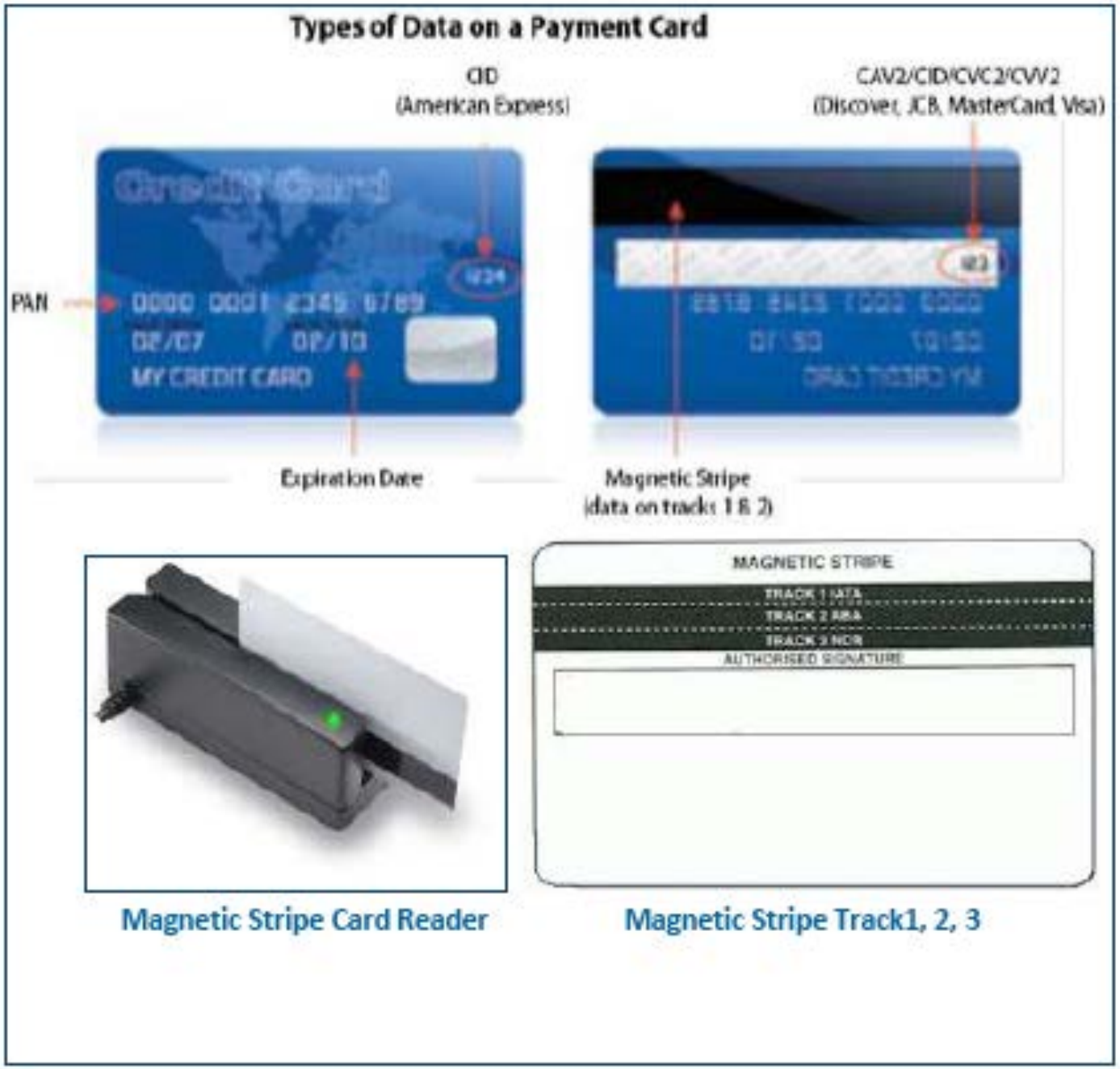



# “Not-so-smart” Magnetic Stripe Cards



- Invented by IBM in 1969
- Three tracks: 1 & 3 at 210 bits/inch; 2 at 75 bpi
- Start sentinel (1 char): %
- Format code (1 char): B for bank/financial
- PAN, Primary Account Number (19 char)
  - Major industry identifier (1 or 2 char): 4, 5 for credit cards
  - Issuer (up to 5 char)
  - Individual account number (up to 12 char)
- Field separator (1 char): ^
- Name
- Field separator
- Expiration date (4 char): YYMM
- Proprietary fields, including Pin Verification Value (PVV)
- Authorization: **Online Only**

# “Not-so-smart” Magnetic Stripe Cards



# “Not-so-smart” Magnetic Stripe Cards

**Banking Specific (Payment Cards)**

1. Financial Information:
    1. Card Information, Stored in card & Card Management System
        1. PAN (Primary Account Number – 16/19 digits)
        2. Expiry Date
        3. CVV (stored in magnetic stripe) – Used for Card Present Transaction
           CVV2 (printed at card) – Used for Card Non Present Transaction
    2. Account Information
        1. Linked to Saving / Checque / Credit Card Account (Unsecured Loan)
2. Information Stored (Plain Text):
    1. Track1
    2. Track2
    3. Track3
3. Standards: ISO/IEC 4909, 7810, 7811, 7812, 7813, 4909, 8583
4. Reference https://en.wikipedia.org/wiki/Magnetic_stripe_card

# Magnetic Stripe Examples

**Track 1:**

```
%B1234567890123445^PADILLA/L.                ^99011200000000000000**XXX******?*
^^^                 ^^                       ^^   ^       ^         ^        ^^
|||_ Card number  ||_ Card holder            ||   |       |         |_ CVV** ||_ LRC
||_ Format code   |_ Field separator          ||   |       |                  |_ End
sentinel
|_ Start sentinel           Field separator _||   |       |_ Discretionary data
                                 Expiration _|   |_ Service code
```

**Track 2:**

```
;1234567890123445=99011200XXXX000000000?*
^^                ^^   ^   ^           ^^
||_ Card number  ||   |   |_ Encrypted||_ LRC
|_ Start sentinel||   |      PIN***   |_ End sentinel
                 ||   |_ Service code
Field separator _||_ Expiration
```

**Track 3:**

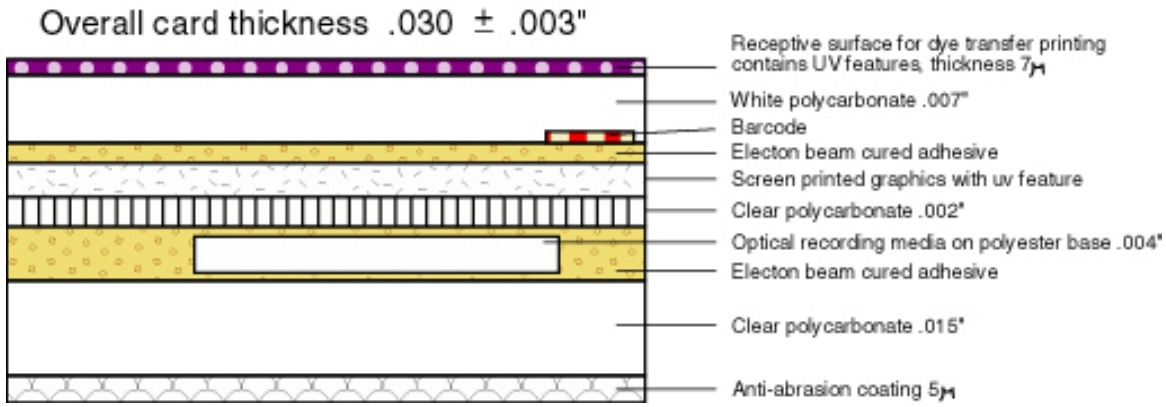
```
;0112345678901234 45=724724100000000000030300XXXX040400099010=************************==1=0000000000000000?*
^^ ^                ^^  ^  ^            ^ ^  ^   ^^ ^   ^    ^^                       ^^^^^                ^^
|| |                ||  |  |_ Currency  | |  |   || |   |    ||_ First subsidiary     |||||_ Additional   ||
|| |                ||  |     exponent  | |  |   || |   |    |   account number (FSAN)|||||   data          ||
|| |_ Card number   ||  |_ Currency     | |  |   || |   |    |_ Field separator       ||||_ Field         ||_ LRC
||_ Format code     ||     (Peseta)     | |  |   || |   |_ Expiration                 |||   separator     |_ End sentinel
|_ Start sentinel   ||_ Country (Spain) | |  |   || |_ FSAN service restriction      |||_ Relay marker
                    |_ Field separator  | |  |   ||_ PAN service restriction         ||_ Field separator
                         Cycle length _| |  |   |_ Interchange control              |_ Field separator
                            Retry count _|  |_ Encrypted PIN***
```

Source: http://sagan.gae.ucm.es/~padilla/extrawork/magexam1.html

# Laser Optical Memory Card

Capacity: 1MB - 1GB

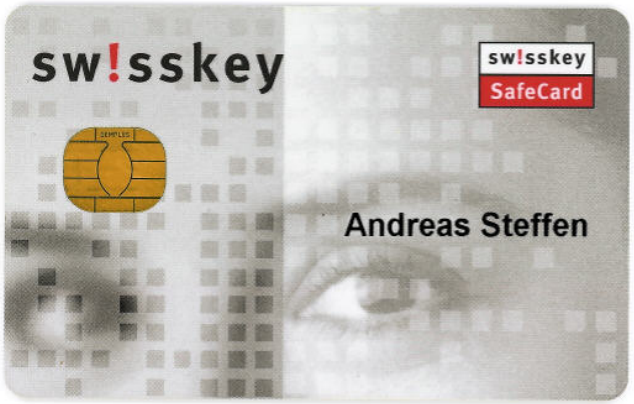




# Other Smart Card Types

SIM card


USB token




Crypto card


Memory card


Java card

SOURCE: ANDREAS STEFFEN

# Other Smart Card Types

dCVV


OTP

OTP key-board

dyn. mag. stripe

display card


multi card emulation

display / BLE

LED

biometrics

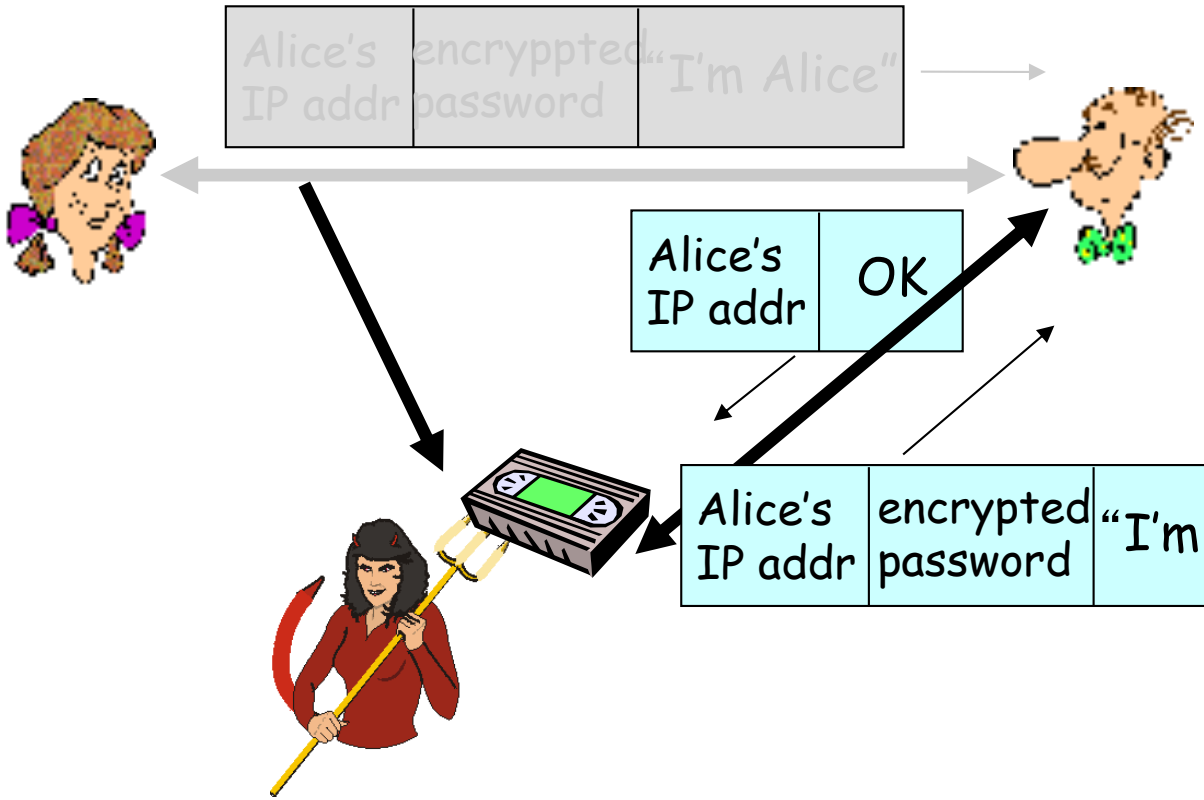
BDR eID

Source: LINXENS

# Hong Kong Smart ID

# Why a Microprocessor-embedded Smart Card ?
# Recall: Pitfalls of Authentication Handshake

Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.

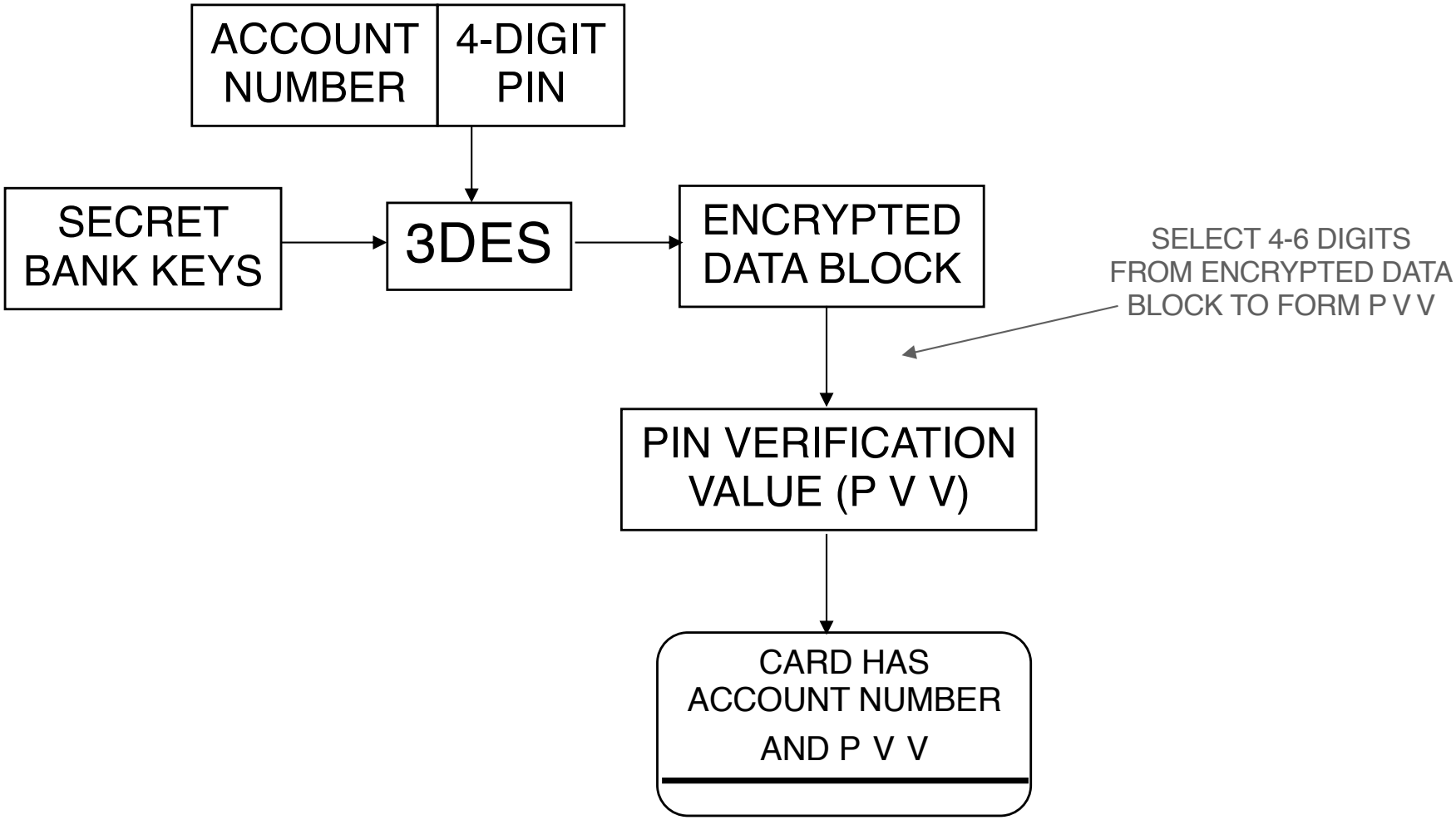



record and playback still works!

# Sample Use Case of a Not-so-Smart Card: ATM and Debit Card Cryptography

- PIN cannot be stored anywhere in plaintext
- PIN cannot be reverse-engineered from the card or any database
- Generate a random 4-digit number (the PIN)
- Combine PIN with other data (account number) to form a data block
- Encrypt the data block using 3DES and secret bank keys
- Select several digits from the encrypted data to use as the Pin Verification Value (PVV)

# Forming the Pin Verification Value



# Using the Card


CARD HAS ACCOUNT NUMBER AND PVV

ATM MACHINE READS ACCOUNT NUMBER AND P V V

USER TYPES PIN

MACHINE NOW HAS:

| ACCOUNT NUMBER | 4-DIGIT PIN | P V V |
|---|---|---|

P V Vs MATCH?
USER IS AUTHENTIC

P V Vs DIFFERENT?
USER IS REJECTED

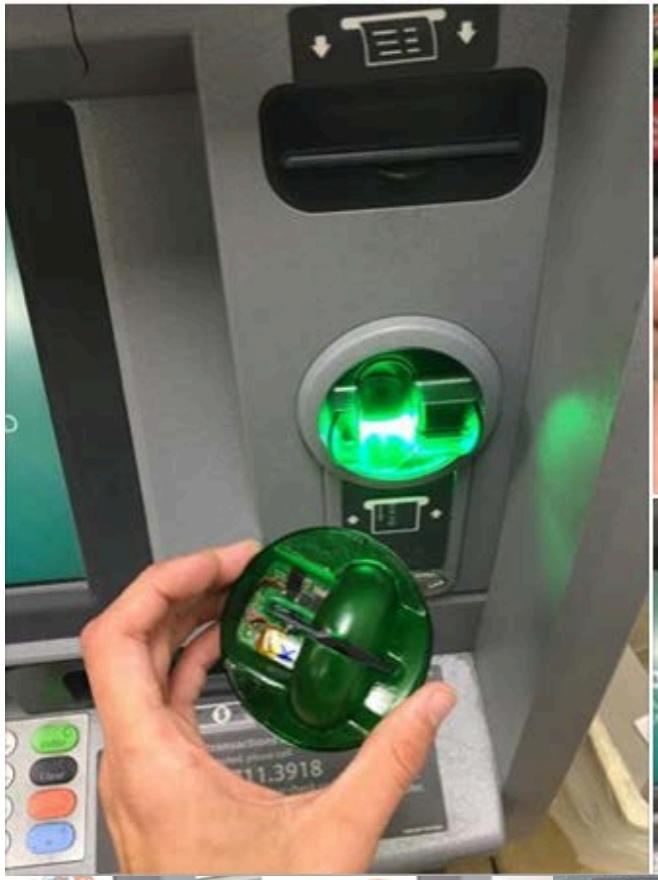
COMPARE CARD P V V WITH COMPUTED P V V

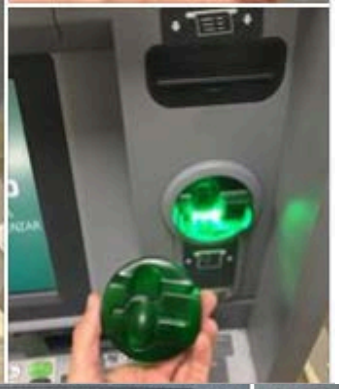
MACHINE HAS BANK KEYS IN HARDWARE:

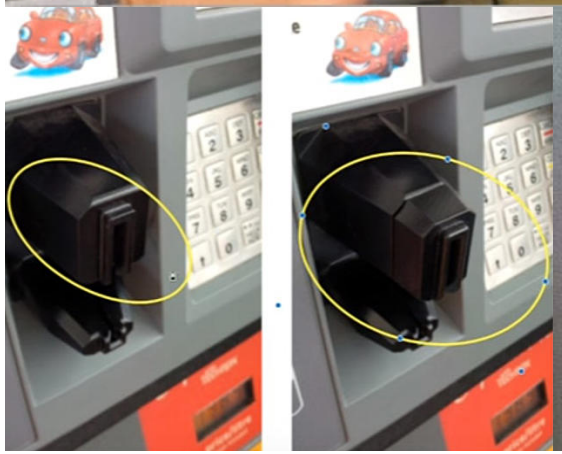
SECRET BANK KEYS → 3DES → DECRYPTED DATA BLOCK → P V V

COMPUTE P V V

# Skimming Magnetic Stripe Cards





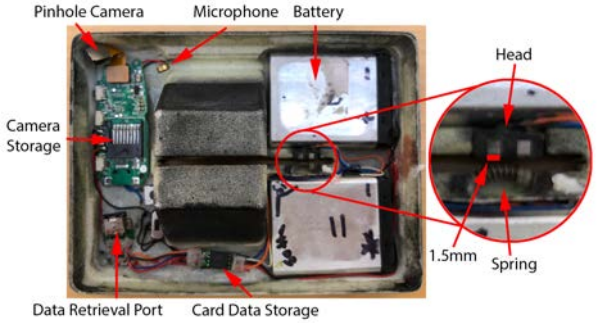



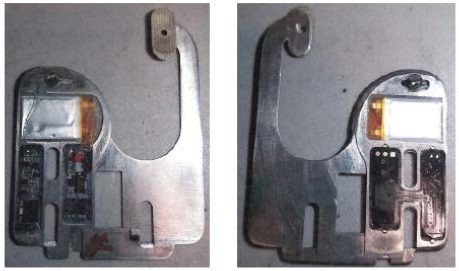


| Location / Type | ATM | Gas Pump | POS Terminal | Total |
|---|---|---|---|---|
| **Bank** | | | | **12** |
| Deep Insert | 10 | | | |
| Shimmer | 2 | | | |
| **Gas Station** | | | | **6** |
| Internal | | 5 | | |
| Overlay | 1 | | | |
| **Hotel** | | | | **3** |
| Overlay | 2 | | | |
| Wiretap | | | 1 | |
| **Restaurant** | | | | **5** |
| Overlay | 5 | | | |
| **Retail** | | | | **9** |
| Deep Insert | 1 | | | |
| Overlay | 5 | | 3 | |
| **Total** | 26 | 5 | 4 | **35** |

Table 1: The breakdown of skimmer BOLOs by the NYPD Financial Crimes Task force between 2016-Jul-14 and 2017-Nov-11. ATMs were the most widely attacked device using both deep-insert and overlay skimmers.

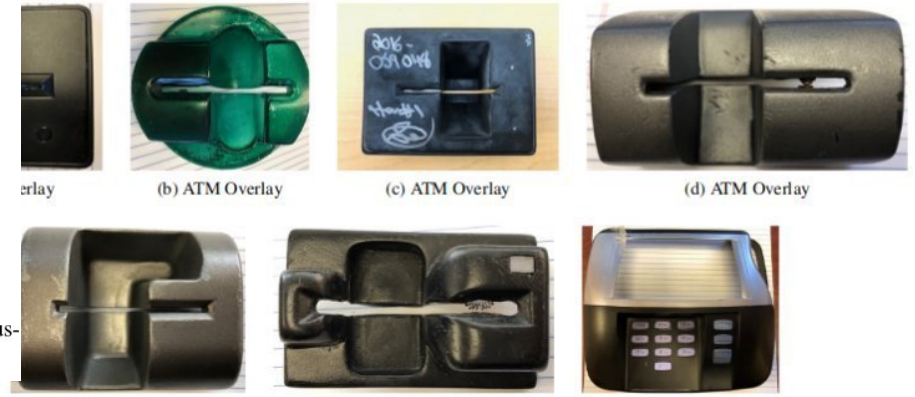
# Card Skimmers Internals



(a) Top (b) Bottom

Figure 7: This deep-insert skimmer is machined to a custom fit for the targeted payment terminal.



erlay (b) ATM Overlay (c) ATM Overlay (d) ATM Overlay

(e) ATM Overlay (f) ATM Overlay (g) POS Overlay

(a) Front (b) Rear (c) Installed

Figure 3: The front and rear of a typical overlay skimmer along with a photo of the skimmer installed on a real ATM, as captured by the NYPD. From the rear, the hardware for reading and storing the card data can be seen.

(h) ATM Door Access Overlay (i) Deep-Insert (j) Deep-Insert


(a) PIN Pad Overlay (b) Reverse


Figure 4: This is a frame of video captured by a camera deployed alongside a skimmer. The adversary uses the camera to capture the victim's PIN upon entry. With both card data and the PIN, the card can be used to obtain cash.

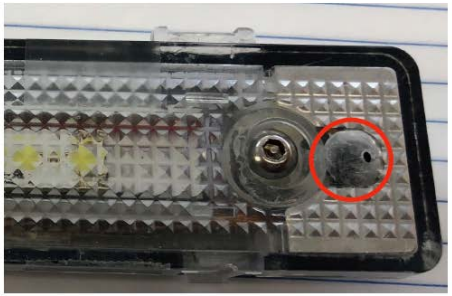


Figure 5: Adversaries modify original ATM light fixtures with pinholes for cameras, such as the one circled in red.

capture cards for months before detection.

### 3.2 Targets

Source:

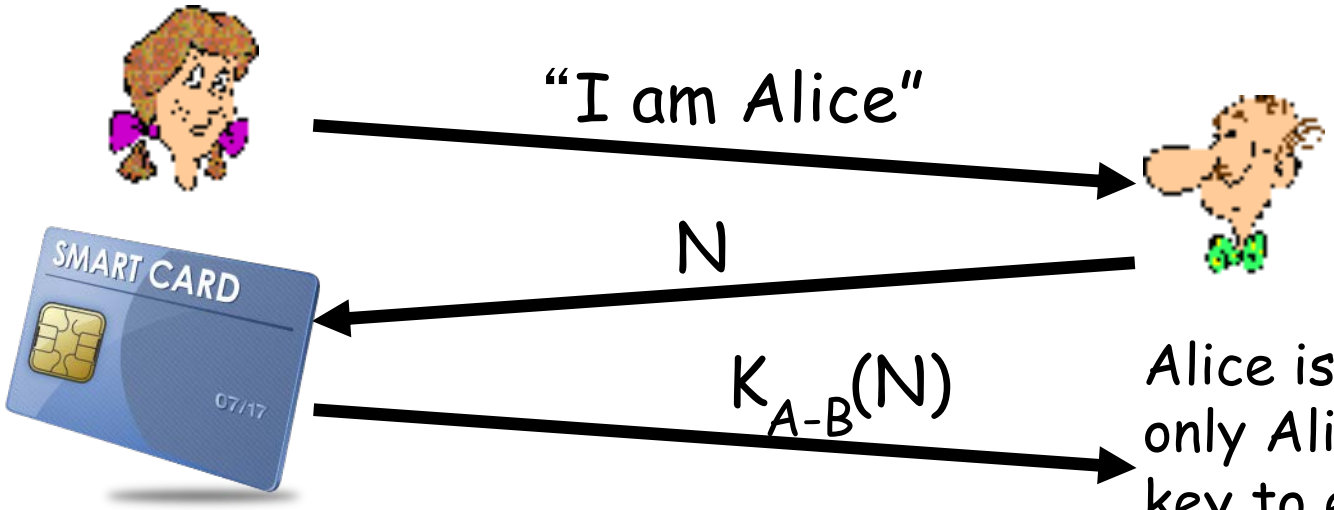
N. Scaife et al, "Fear the Reaper: Characterization and Fast Detection of Fast Card Skimmers" Usenix Security 2018

# Card with Embedded-Microprocessor to enable Challenge-Response Handshake for Authentication:

Goal: Avoid playback attack

Nonce: number (N) used only *once -in-a-lifetime*

ap4.0: to prove Alice "live", Bob sends Alice nonce, N. Alice must return N, encrypted with shared secret key




The Smartcard's embedded microprocessor can perform the necessary computation to produce the required response WITHOUT disclosing the user key/ PIN to the outside world !

# A Prime Example: the EMV chip cards

EMV stands for **E**uropay, **M**asterCard and **V**isa, a global standard for inter-operation of integrated circuit cards (IC cards or "chip cards") and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions.


**Key Security Advantages:**

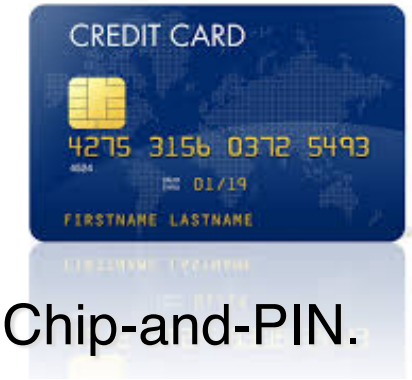
- **Information stored in a more secure microprocessor chip**
  - Instead of a less secure magnetic stripe
- **Personalization of EMV cards is done using issuer-specific keys**
- **Card creates unique transaction data**
  - Any captured data cannot be used to execute new transactions (prevents card skimming and card cloning)
- **Cardholder verification**
  - Terminal will prompt the customer to sign (Chip and Choice in US) or enter a PIN (Chip and PIN in EU and is most common in other countries) to validate their identity.
  - Also supports other cardholder verification methods: offline PIN, online PIN, signature, or no cardholder verification method.

# 2 Ways of accepting EMV Chip Card Payments

- **Contact ("dipping" the card):**
  - Cardholder inserts card into POS device. Card remains in device until completion of the transaction. If customer removes card before the charge is approved, the transaction will fail and the customer will be required to provide the card again.

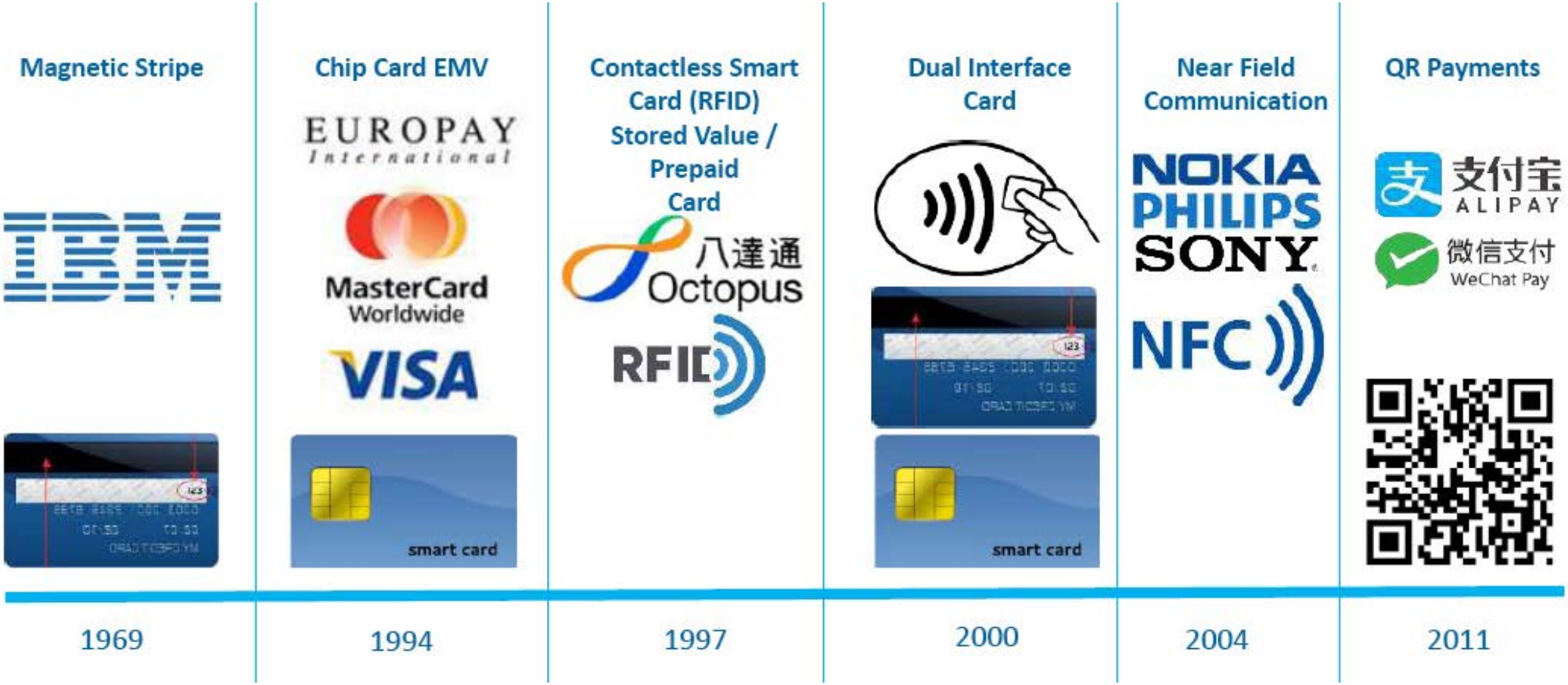
- **Contactless ("tap-and-go", e.g. Visa's PayWave):**
  - Cardholder waves the card by the chip card-enabled POS device to provide payment information. Once the transaction has been authorized, customer might then be prompted to enter PIN or sign a receipt, or no verification is needed if the amount is below certain threshold (e.g. < HK$300).


# EMV chip cards Adoption




- The European Union was the first to Mandate the support of Chip-and-PIN.
- Deployment in US was lagging behind because US companies claimed that they already had enough Credit Card security/ Fraud detection mechanisms in place and they were reluctant to incur the large cost (est. US$12 billion) of deploying such new technologies.
  - But some high-profile security breaches invalidated such claims, e.g.
    - In late 2013, Target's system got hacked and lost 40 million credit/ debit card numbers of its customers, together with 70 millions of customer records.
- In October 19, 2014, President Obama signed executive order to speed up the adoption of EMV cards in the US by October 2015.
  - Newly issued and existing government credit/ debit cards would have chip technology.
  - All POS terminals at federal agencies would accept EMV.

# Payment Media Evolution



# Liability Shift after EMV


- Before EMV, POS counterfeit fraud is largely absorbed by Card Issuers
- Starting October 2015: Card Brand Networks' Liability Shift
  - *The party, either the issuer or merchant, who does not support EMV, assumes liability for counterfeit card transactions.*

**Counterfeit Fraud Liability Shifts**
Rewards investment in EMV
POS: October 1, 2015
AFD & ATM: October 1, 2017

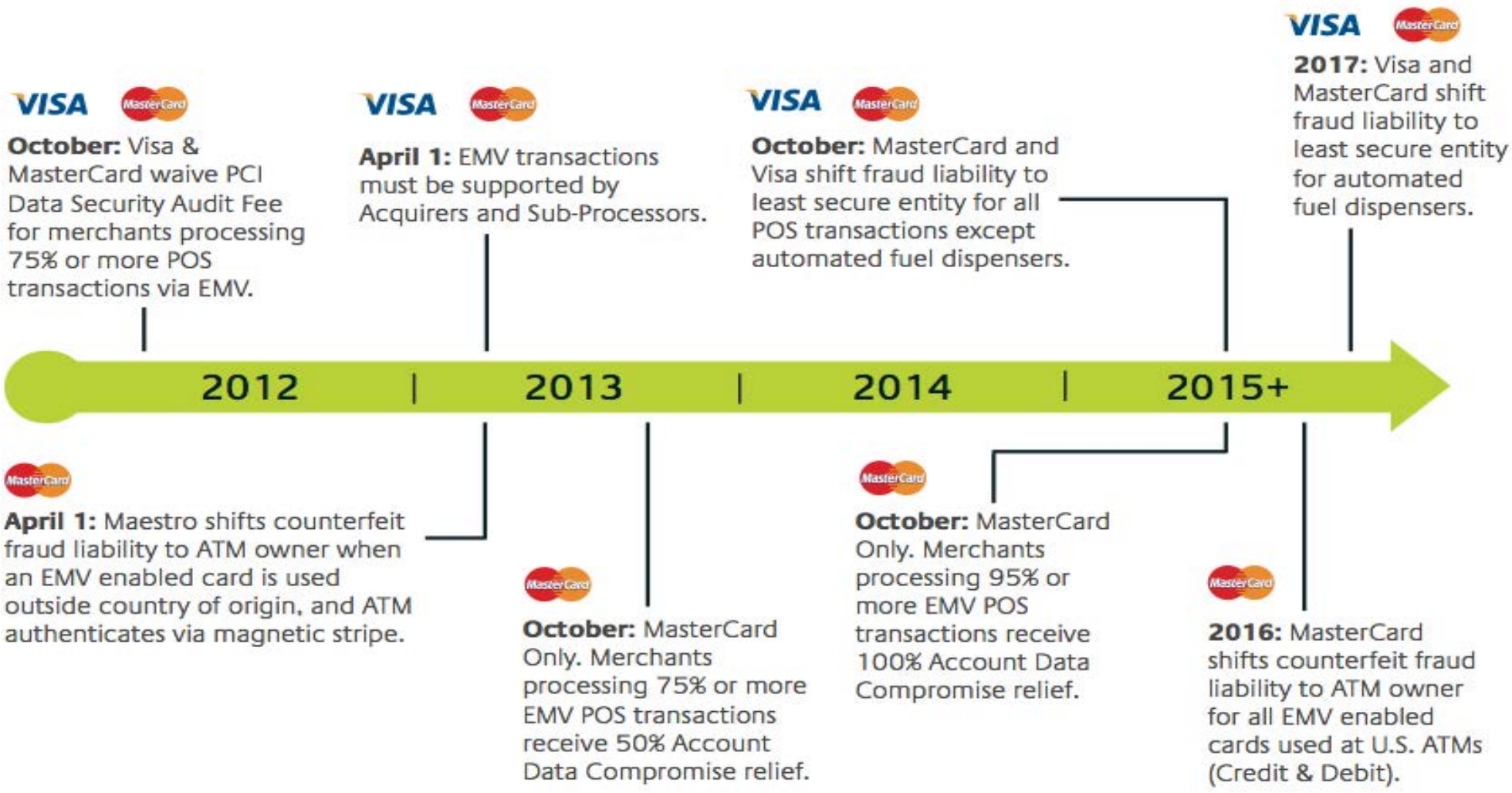
- After Liability Shift: Liability shifts to the acquirer if ***counterfeit fraud*** occurs on a contact chip capable card and the merchant is not contact chip capable
- Liability Shift does ***not*** apply to contactless, card-not-present transactions, or lost/stolen fraud
- Covers domestic and cross-border transactions

| Transaction Examples | Counterfeit Liability |
|---|---|
| Chip-on-chip transactions | Issuer holds the limited exposure that still exists |
| Mag-stripe cards at chip terminals | Issuer holds liability |
| Contact chip at mag-stripe terminals | Acquirer holds liability |

# Merchants Reliefs vs. Costs


- Relief from requirement to submit PCI compliance validation documentation (PCI security standard compliance cost ~ US$2K/yr vs. US$700/yr Card fraud cost at each store)
  - Effective Oct. 1, 2015, relief from financial liability for card-present fraud losses processed on EMV terminals.
  - Fuel-selling merchants had until Oct 1, 2017, before liability shift took effects at Automated Fuel Dispensers (AFD, i.e. Fuel Pumps), due to added expenses of updating (Ave cost for EMV conversion: US$6-10K per pump)
- Liability shift was also introduced for ATM transactions in the U.S. Oct 2016-2017
  - All ATMs needed to be EMV compliant
  - After October 2016/2017, FIs could hold ATM operators liable for fraudulent withdrawals and cash advances from debit and credit cards.
  - Approximately US$2,000 to upgrade an ATM to be EMV-capable (Aite)
    - Some ATMs could not take the upgrade for EMV and/or Windows (move from XP); US35k+ for a new ATM

# Key EMV dates from Card Brands



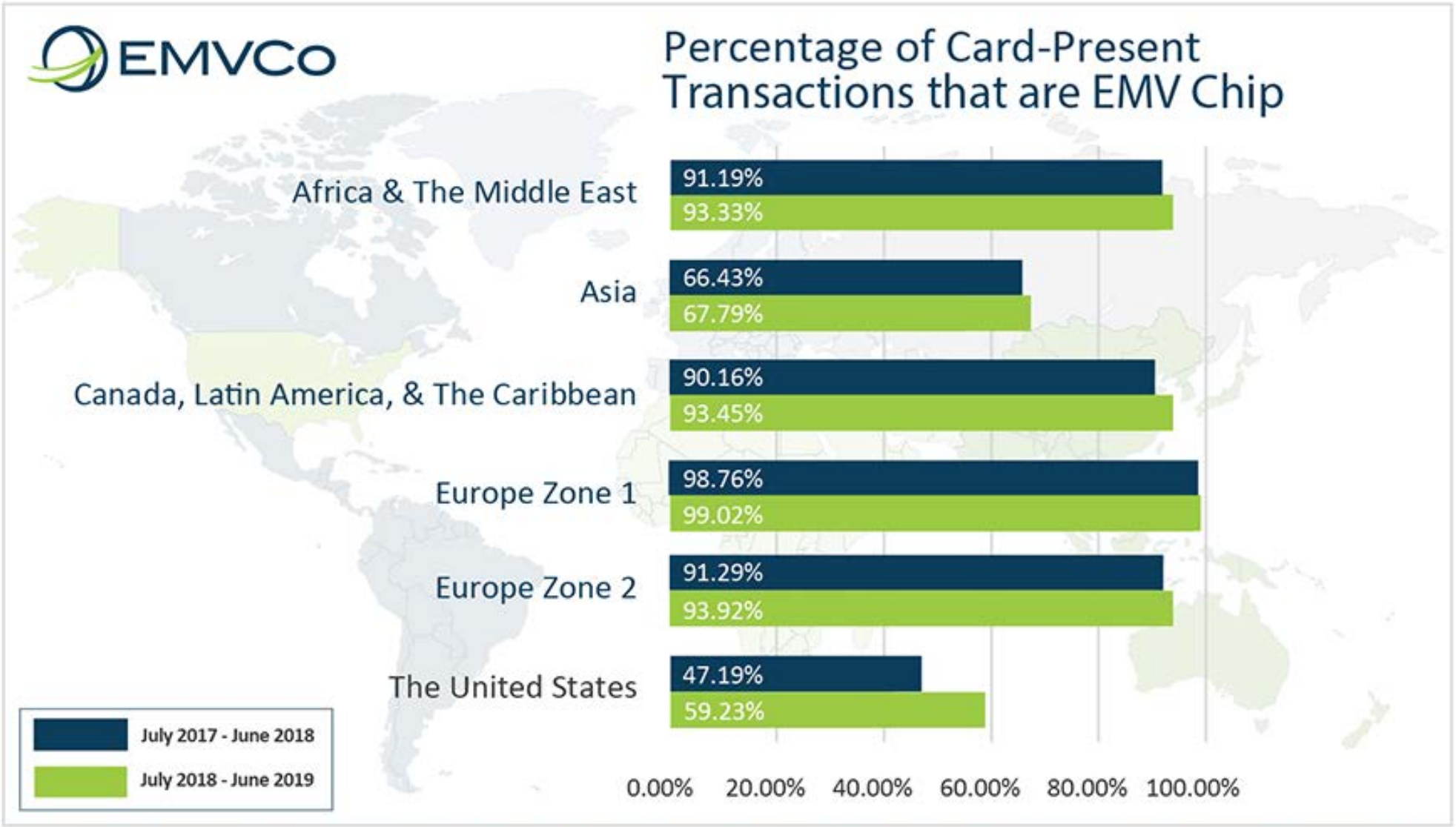

State Employees' Credit Union®

*There is a Difference!*

# Worldwide EMV Chip Card Deployment and Adoption*

| | 2016 | | 2017 | | 2018 | |
|---|---|---|---|---|---|---|
| Region | EMV Cards | Adoption Rate | EMV Cards | Adoption Rate | EMV Cards | Adoption Rate |
| Africa & the Middle East | 184M | 68.7% | 219M | 74.8% | 272M | 87.8% |
| Asia Pacific | 3,331M | 38.8% | 4,147M | 45.7% | 5,001M | 51.0% |
| Canada, Latin America, and the Carribbean | 717M | 75.7% | 820M | 85.7% | 848M | 86.9% |
| Europe Zone 1 | 921M | 84.9% | 939M | 84.4% | 966M | 85.5% |
| Europe Zone 2 | 243M | 63.7% | 276M | 71.4% | 301M | 80.4% |
| United States | 675M | 52.2% | 785M | 58.5% | 842M | 60.7% |

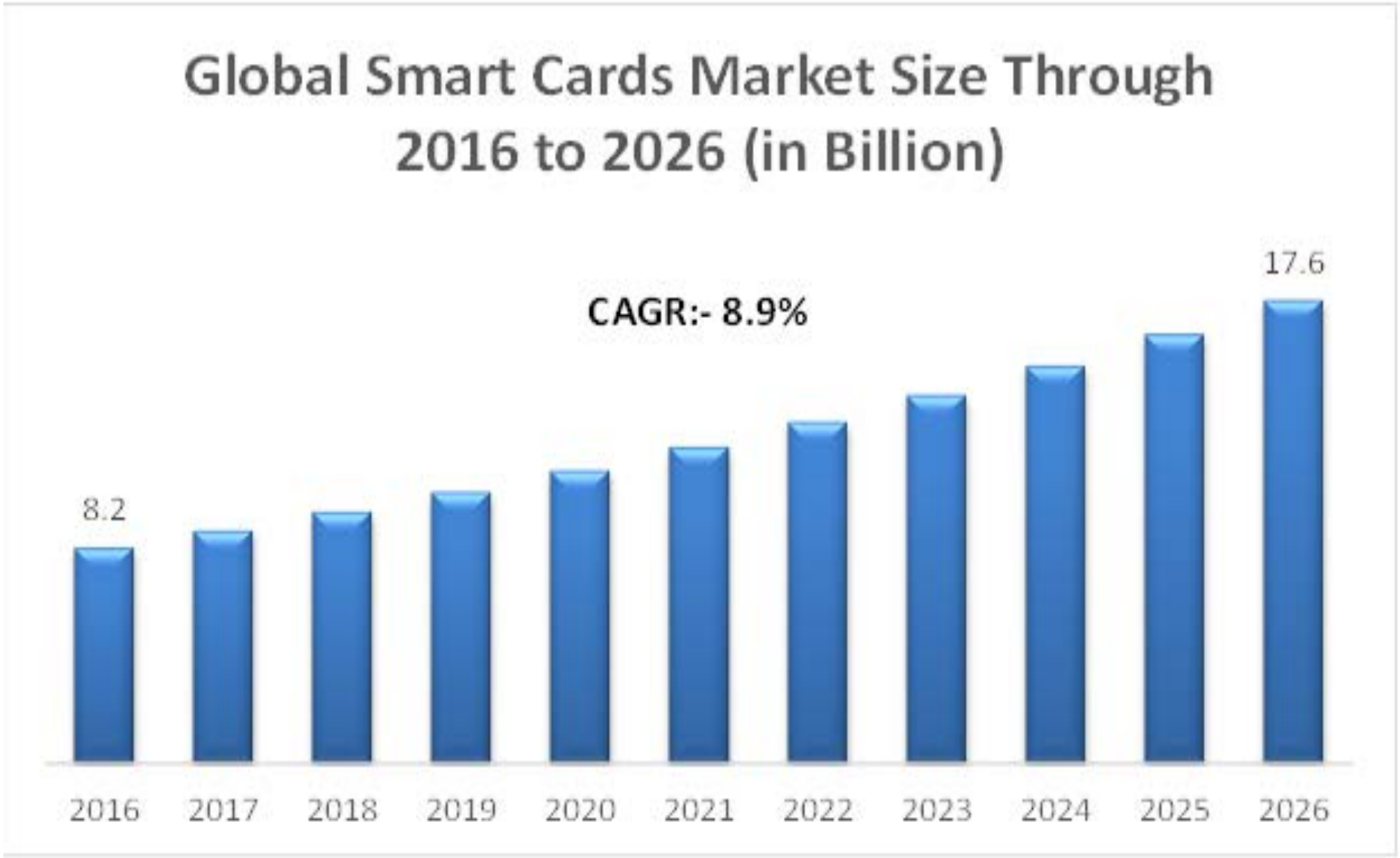
*Figures reported in Q4 of 2016, 2017, and 2018, respectively, and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member institutions globally.




*Data represents the most accurate possible data that could be obtained by American Express, Discover, JCB, Mastercard, UnionPay and Visa for transactions processed by them during the noted period. The transaction data reflects an average of 12 months' data as reported by all members to take into consideration seasonal variations. To qualify as an 'EMV chip transaction', both the card and terminal used during a transaction must be EMV chip-enabled. Data is reported from the acquirer perspective. These figures may not include offline transactions, 'on us' transactions (defined as a transaction handled exclusively by another processor) and/or transactions processed by non-EMVCo member institutions, such as national payment networks.*

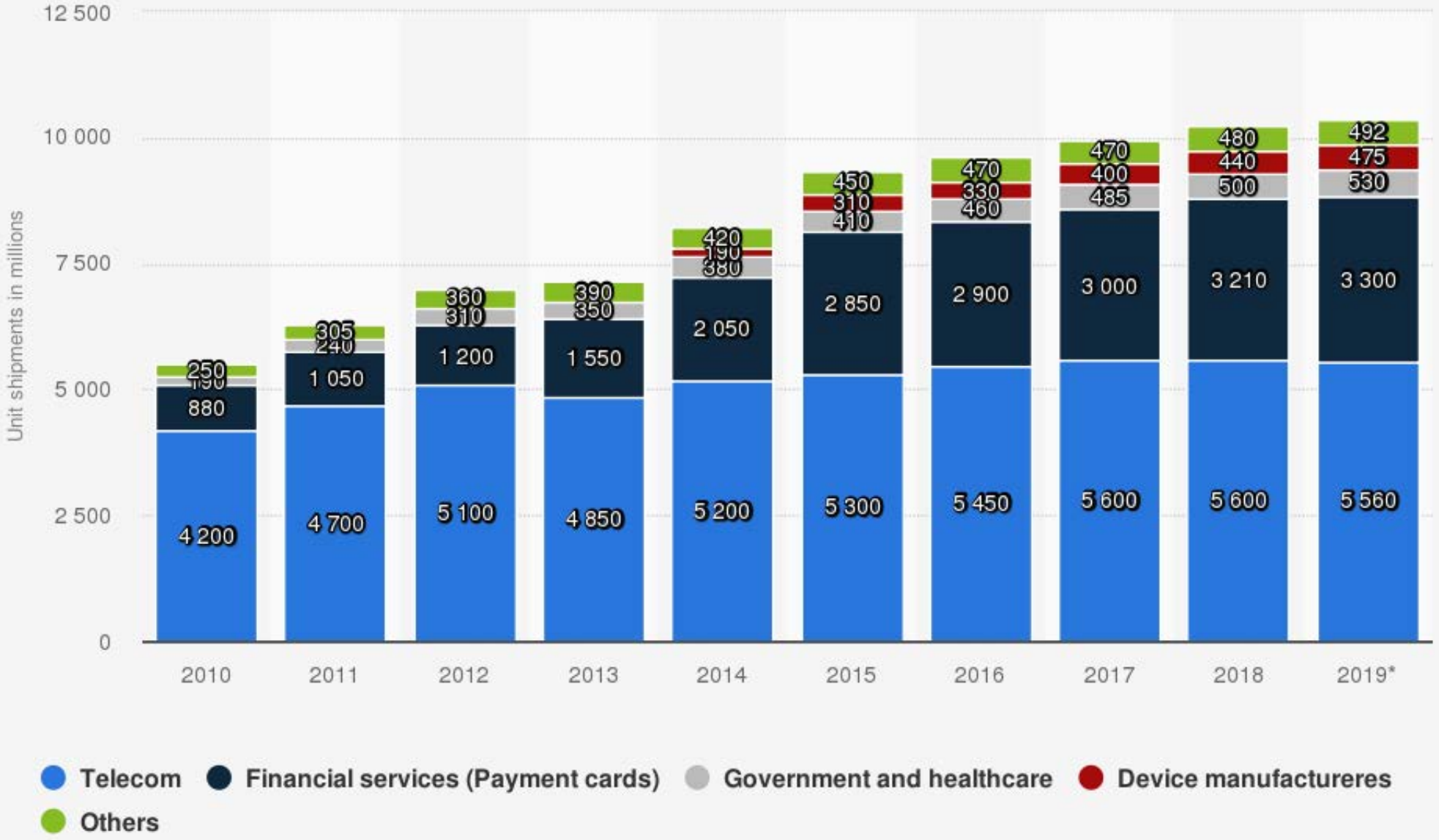
# Examples of Mobile Card Reader Providers

| Provider | Region Available | Magnetic Stripe/EMV | Card Reader Cost | Transaction Fee Options |
|---|---|---|---|---|
| Intuit Go Payments | North America | Magnetic stripe | Free | Per transaction fee, or fixed monthly fee and lower per transaction fee |
| iZettle | Western Europe Latin America | EMV | Free for chip and signature Fee for chip and PIN | Per transaction fee |
| mPowa | Global | EMV | Fee for chip and PIN | Per transaction fee |
| PayAnywhere | North America | Magnetic stripe | Free | Per transaction fee |
| payleven | Western Europe Latin America | EMV | Fee for chip and PIN | Per transaction fee |
| PayPal Here | North America | Magnetic stripe | Free | Per transaction fee |
| Square | North America | Magnetic stripe | Free | Per transaction fee or fixed monthly fee |
| SumUp | Western Europe | EMV | Free | Per transaction fee |




Source: Maximize Market Research

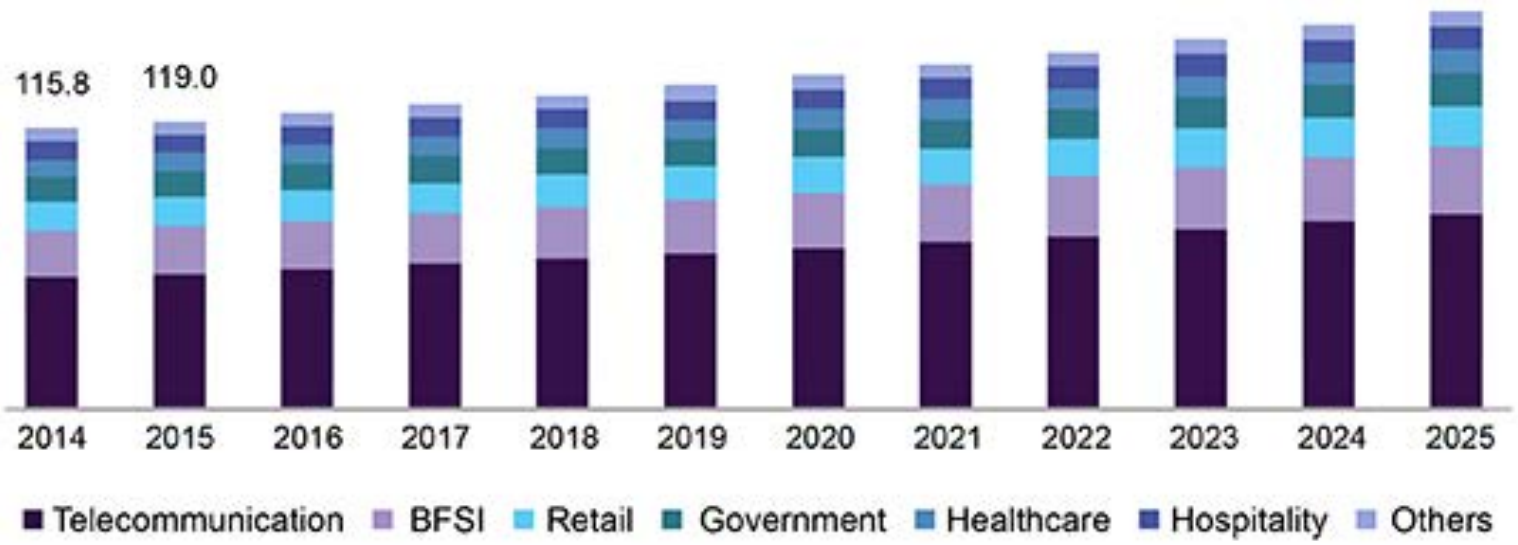
# Secure elements shipments worldwide from 2010 to 2019 (in million units), by vertical



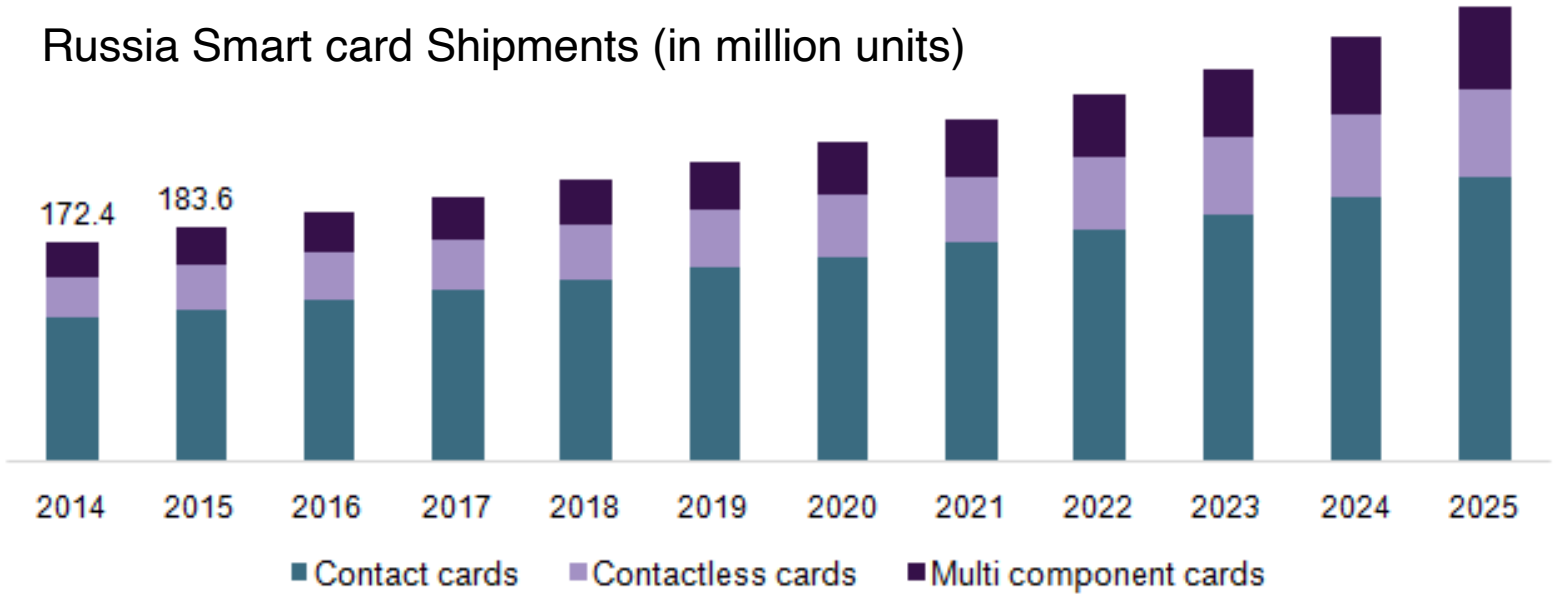

Source
Eurosmart


Additional Information:
Worldwide; Eurosmart; 2010 to 2018

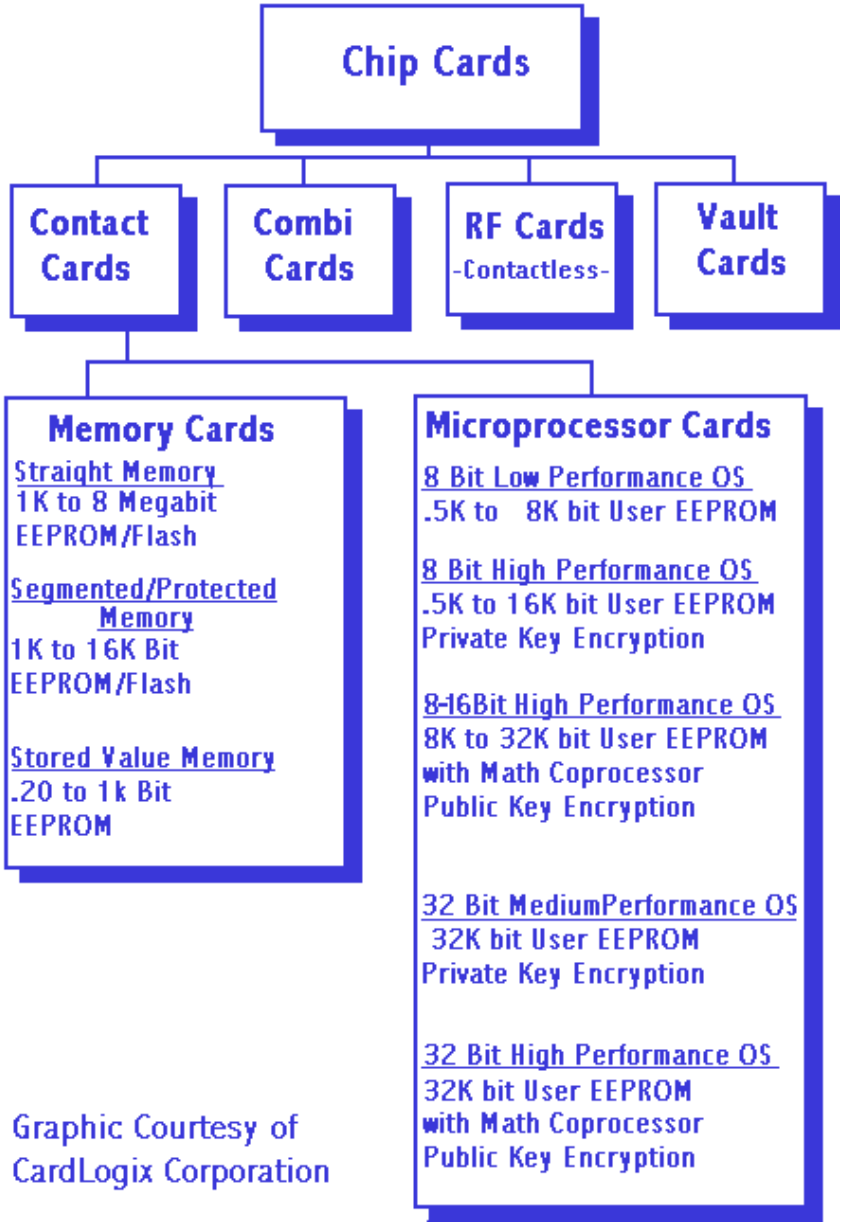
## U.S. smart card materials market size, by application, 2014 - 2025 (USD Million)




Russia Smart card Shipments (in million units)



# Yet another Card Taxonomy (circa 2000)




Graphic Courtesy of
CardLogix Corporation

SOURCE: SMARTCARDCENTRAL.COM

# Wiegand Cards

- Wiegand cards use the Wiegand effect: in cold-worked ferromagnetic wires a signal can cause magnetic fields to reverse suddenly, generating a sharp voltage pulse
- Can encode a card number and other information during manufacture
- When the card is passed through the reader, a sensing coil in the reader picks up the unique pattern.
- Each Wiegand card is programmed with a unique code that is permanent and virtually impossible to copy.
- The cards are also programmed with a site code that distinguishes between different facilities or installations.

# Multi-Application Smart Card

SSL Secure Web

S/Mime Secure Mail

Customer PKI Application

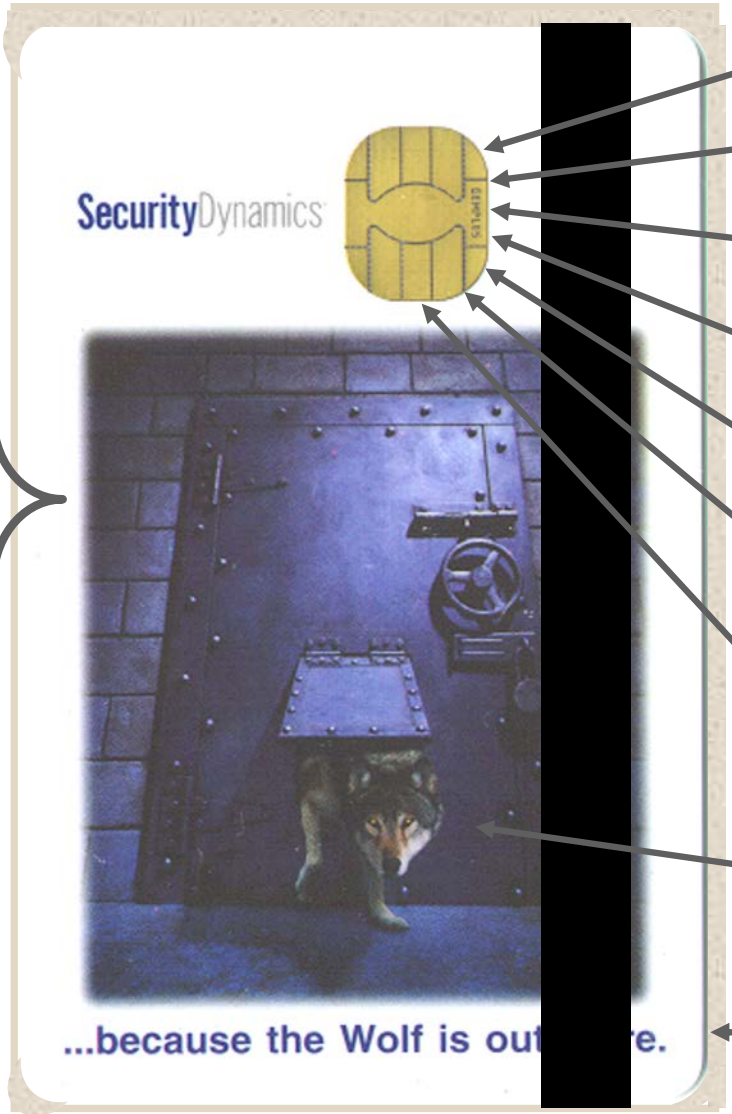
Single Sign-On

Biometric Authentication

Local File Encrypt

Secure Screen Saver

Application Login




Private Key(s)

Digital Certificates

ACE (Active Customer Enrollment) Authentication

Biometric Data

Encryption Key

Employee Data

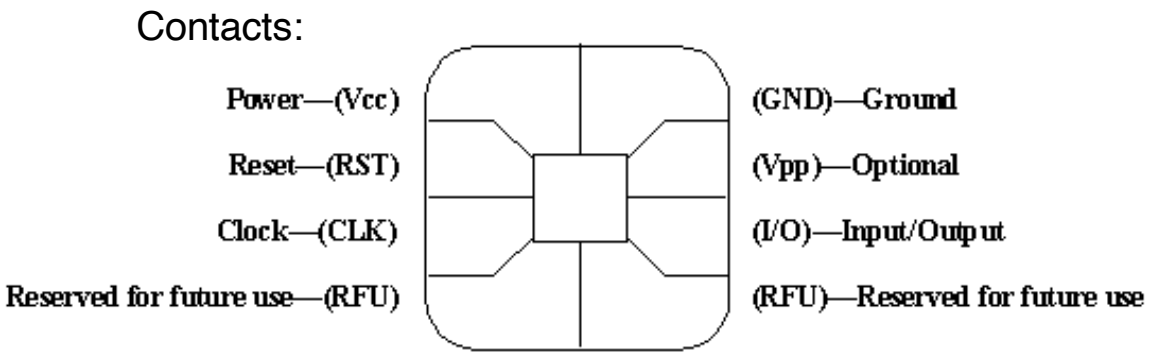
Password Cache

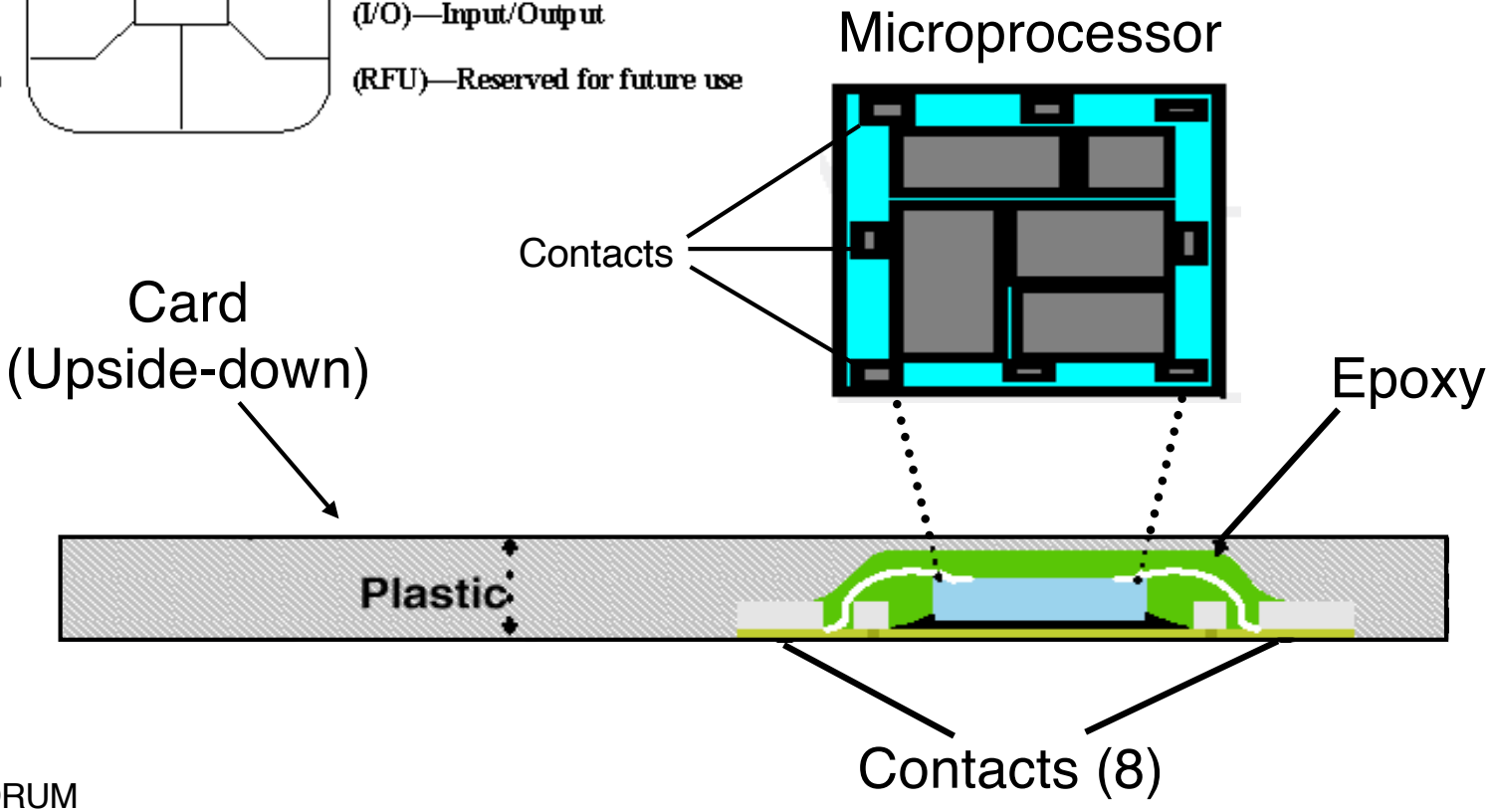
Employee Picture

Magnetic Stripe or RF Door Access

SOURCE: SECURITY DYNAMICS

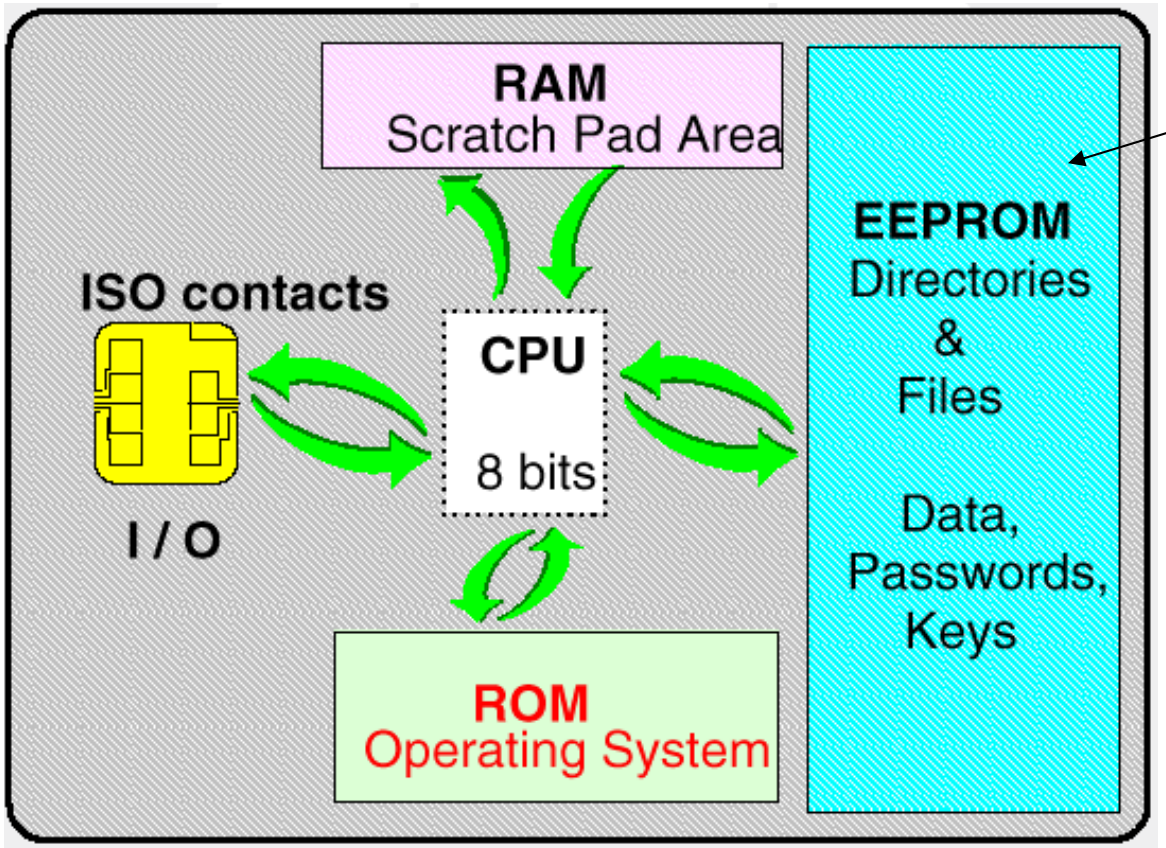
# Smart Card Structure




SOURCE: SMART CARD FORUM

# Old (8-bit) Smart Card Architecture




EEPROM:
Electrically
Erasable
Programmable
Read-Only
Memory

SOURCE: SMART CARD FORUM

# Smart Card Components

Processors

- 8-bit, typical clock speed: 5 MHz (8-bit)
- Optional cryptographic processor

- 32-bit, clock speed 300 MHz

- 64-bit, 600 MHz

SOURCE: SUMIT DHAR

# Smart Card Components

ROM: Read Only Memory

- Used for storing fixed programs. Holds the operating system
- Typically varies from 2KB to around 16 KB
- Once written, cannot be changed
- Occupies the least area

SOURCE: SUMIT DHAR

# Smart Card Components

EEPROM: Electrically Erasable Read Only Memory

- Stores variable data
- Holds various applications and their data.
- Can be read or written to subject to permissions.
- Typically: 2KB to 256 KB

RAM: Random Access Memory

- Used as temporary storage.
- Erased on power off.
- Typically 1000-8000 bytes of data

SOURCE: SUMIT DHAR ; https://www.tech-faq.com/smart-card.html

# Smart Card Standards versus Specifications

- **Official Standards Bodies (e.g. ISO/IEC)**
  - Representatives of both producers and consumers
  - Typically very slow moving, particularly international standards
    - WG4 has been arguing about smart card voltages for years
  - often try to "grandfather in" existing products and thus are overly complex
- **Industry Consortia/Alliance (e.g. MULTOS, JavaCard, OpenCard )**
  - Rally commercial partners around some IP such as a Patent
  - Rules written to exclude particular parties
- **Issuer Consortia (e.g. EMV, CEPS)**
  - EMV (Europay MasterCard Visa) and CEPS (Common Electronic Purse Specifications) are the classic examples
  - proprietary variants tend to short-circuit inter-operability
- **User and Governmental Consortia**
  - not very effective since issuers are in charge

# The Focus of Standards and Specifications

- **Standards homogenize, specifications differentiate**
- **Card-Edge Standards**
  - Enforcement
    - testing, test suites, test standards and certification
    - operational enforcement
- **API Specifications**
  - Documented interface to proprietary “stack”
  - Many underlying levels bound together
  - Don’t de-couple applications from particular vendors
  - Very difficult to tell what happens where behind the API

# Examples of Official Smartcard Standards

## ISO/IEC

- ISO 7816-1 through -15 are core smart card standards
- -1, -2, and -3 deal with the physical (hardware) aspects of smart cards and are observed
- -4 through -9 deal with the functionality (software) aspects of software and are by and large ignored
- ISO/IEC 14443 defines Interface to Close Proximity (~ upto 10cm) Contactless Smartcards, operating at 13.56MHz.
- ISO/IEC 15693 defines standards for “Vincity” cards (~ upto 1m)
- ISO/IEC 18092 Near Field Communications (NFC) Interface and Protocol standards integrated into Mobile phones and other devices
  - Support backward compatibility with ISO/IEC 14443 Type A Contactless Cards as well as similar technologies, SONY FeliCa cards

## ITU/ETSI/3GPP

- official body controlling the Telecommunications standards, e.g. GSM, 3G, 4G, 5G (which also include the SIM/ microSIM/ nanoSIM standards
- In charge with coordinating all mobile SIMs
- Important for standardizing algorithms and processes in which smart cards are used

## ANSI-INCITS

- Biometric Standards, e.g. face recognition, finger-print, iris, hand-geometry etc, to enhance security and Privacy of ID standards

# Examples of Supplier (Technologies) Specifications

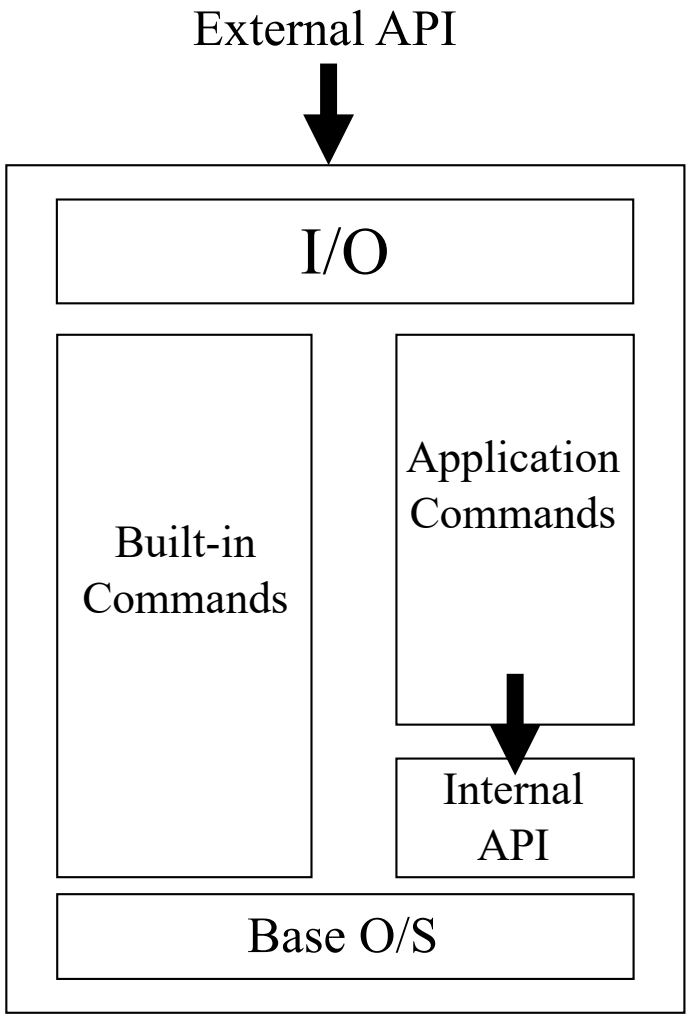
- **MULTOS**
  - perhaps the oldest of the consortia
  - writes very detailed specifications for implementers of the Multos card which have delivered interoperable cards from multiple vendors
- **PC/SC**
  - specifications for attaching smart card readers to personal computers and workstations
  - compliance realized through a testing and certification process
- **Java Card Forum**
  - feeds recommendations for evolution of Java Card to Oracle
- **OpenCard Framework, PKCS, SIM Alliance, ...**

# Examples of Issuer Specifications

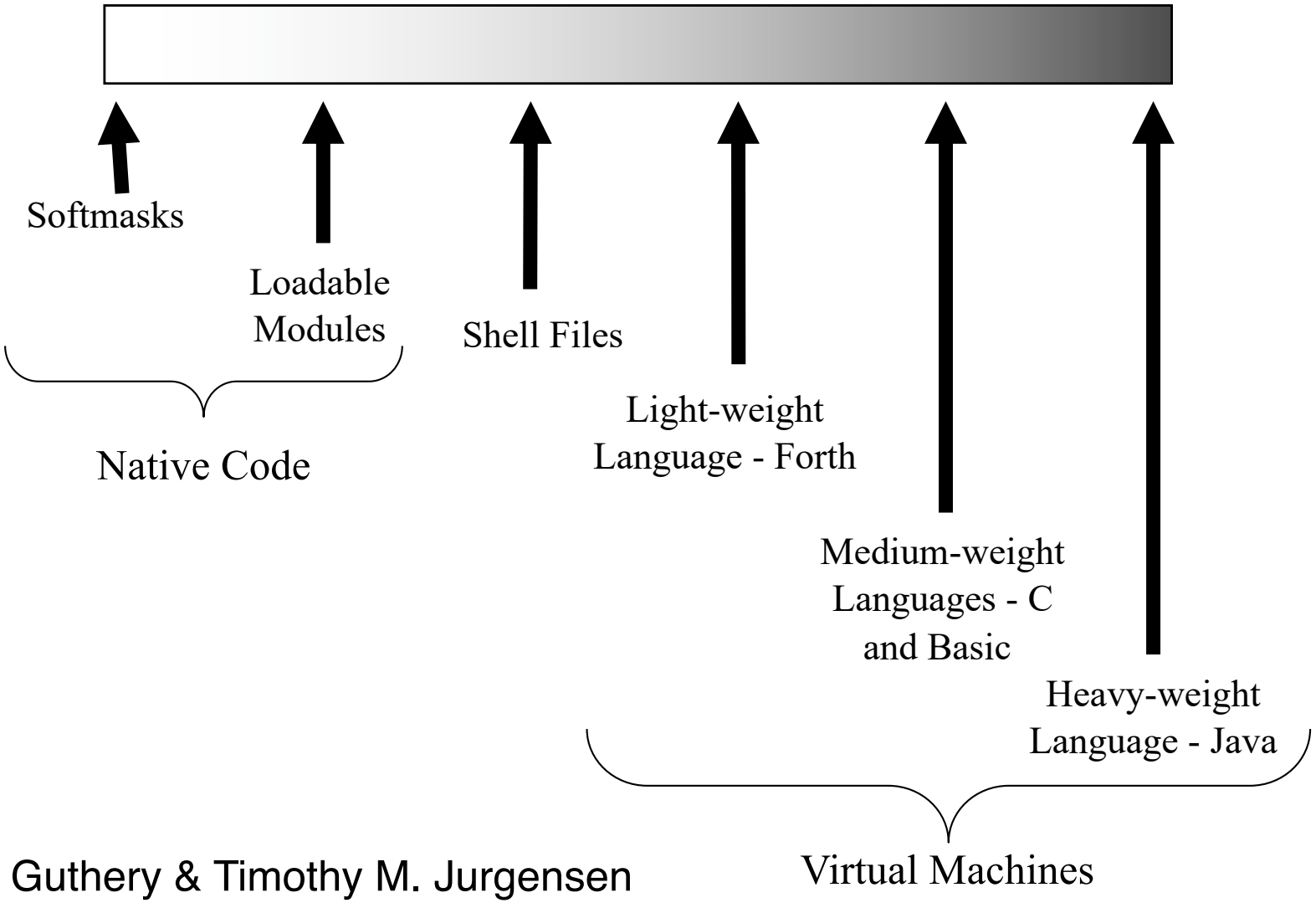
- **EMV**
  - Multi-(credit/debit)-application architecture
  - A card-edge specification which includes card and terminal specification
  - Many variants exist (UKIS, VSDC, MCHIP)
- **G8 Health Standards**
  - Populating Personal medical info on Health card
- **ICAO (International Civil Aviation Organization)**
  - Machine Readable Travel Documents, e.g. ePassports
- **IATA (International Airline and Transportation Assoc)**
  - Smartcard-based ticketless travel

# Software Architecture of a Smart Card

*Built-in commands include a load application command*



# Card-Side Programming



# Softmasks

- Written in or compiled to native code
- Hook into the O/S loop at defined points
  - input byte, buffer full, pre-output, post-output, etc.
- Call O/S low-level routines
- Easy to add a command or modify an existing one
- Touching the manufacturer's "private parts"

# Loadable Modules

- Written in or compiled to native code
- Well-defined (and modest) API - mostly the underlying commands; i.e. module is an on-card application
- Module “framework” of defined entry points
- Loading process varies from card to card
- Techniques for machine code verification can be applied

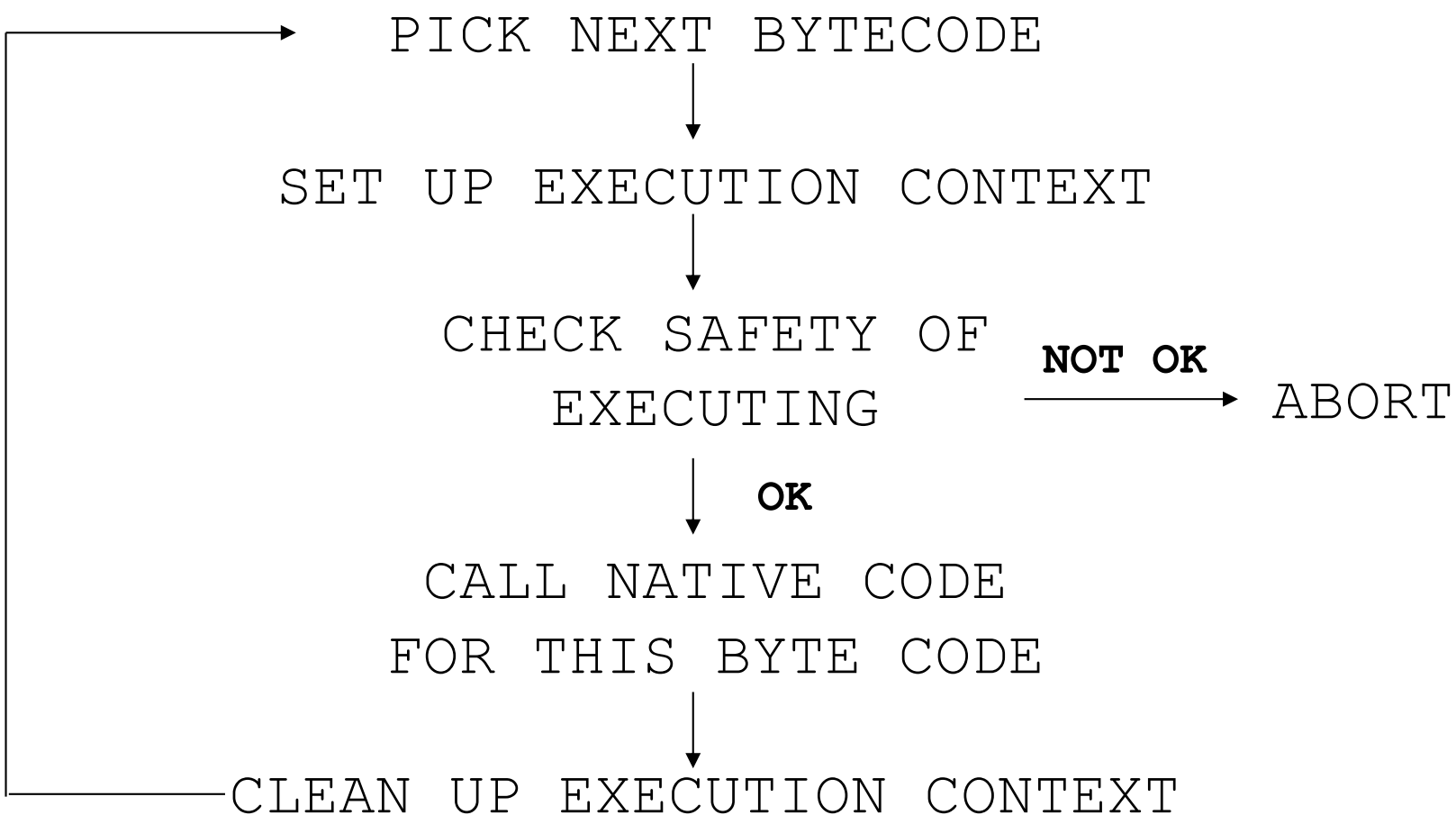
# Virtual Machines

- Written in or compiled to VM byte code
- VM is typically a stack machine of some sort

```
PUSH A
PUSH B
ADD
```

- 20 to 200 times slower than native depending on amount of checking
- API between commands and low-level

# VM Inner Loop



# Java Card

- 18 ISO-7816 commands recast as 51 Java classes with 113 entry points
- Essentially an on-card version of OpenCard
- Partially defines a virtual ISO-7816 card
- No specification of search paths, security status modifications, file names, etc.
- Adds new non-ISO-7816 commands and data constructs

# MULTOS C

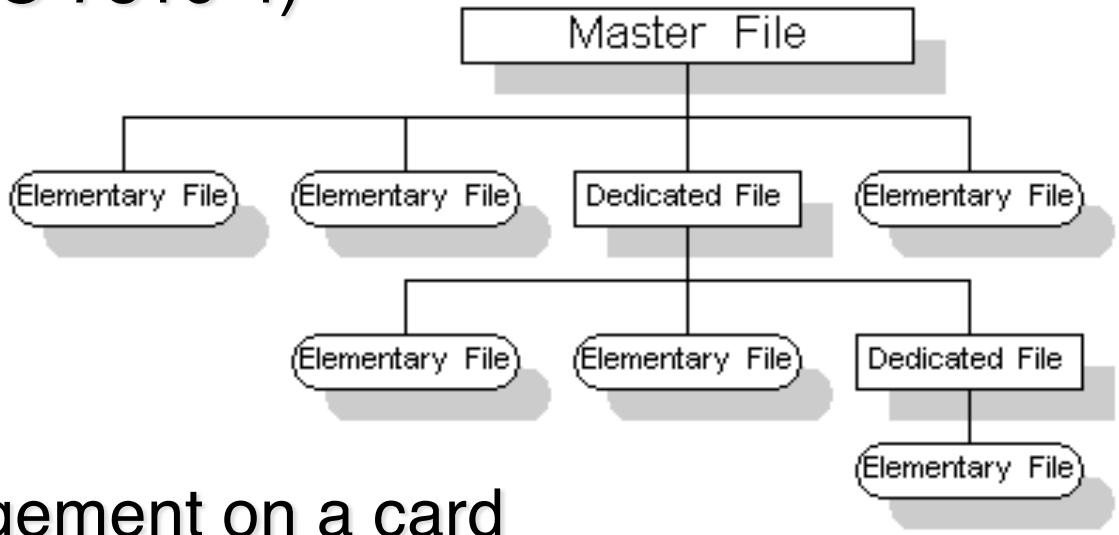
- Non-ISO-7816 operating system built for high-level languages
- C language runtime library file system semantics
- Mix (virtual) assembler and C

# Basic Card

- ISO-7816-4 command template
  - build compliant ISO-7816 commands or roll your own
- Full-bodied Basic
  - volatile and non-volatile data
  - on-card P-code virtual machine
- T=1 communication with encryption
- Call *by reference* from host to card!

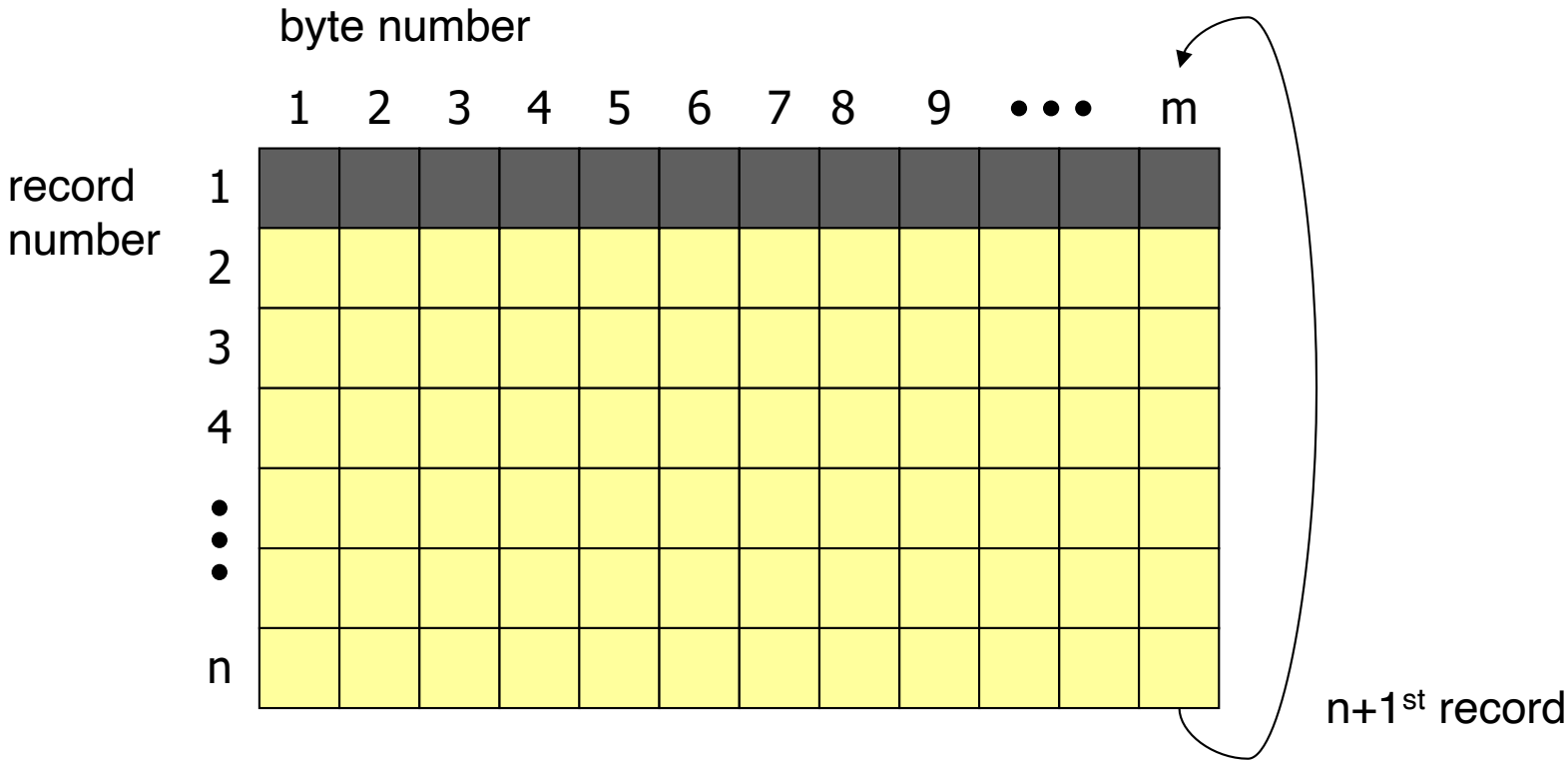
# Smart Card Filesystem/ Database

- File structure (ISO 7816-4)
  - Cyclic files




- Database management on a card
  - SCQL (Structured Card Query Language)
  - Provides standardized interface
  - No need to know file formatting details

# Cyclic File

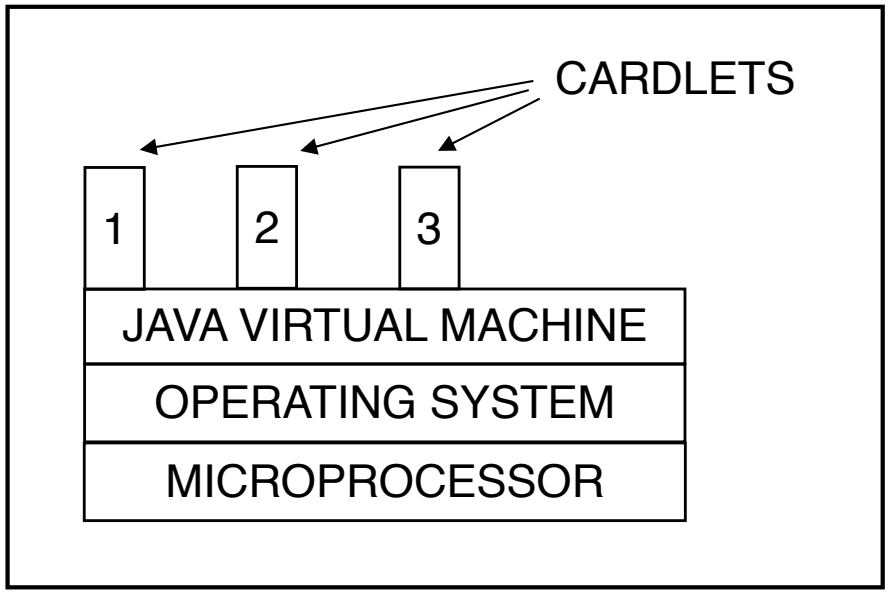



- READ gives the most recently written record
- Maximum number of records: 254
- When maximum is reached, first record is overwritten
- Record length: 1 .. 254 bytes

SOURCE: ANDREAS STEFFEN

# Cyberflex™ Java Smart Card

- Complete 32-bit Java run-time environment on a card
- Utilities for compiling and loading cardlets onto the card from a PC



# The (failed) Java Ring (late 90's)

- Java-enabled iButton
- Communicates by contact at 142 Kbps
- 64 KB ROM and 134 KB RAM
- Stores 30 digital certificates with 1024-bit keys
- Uses: authentication, epayment, access
- Cost: $15-30 in unit quantity

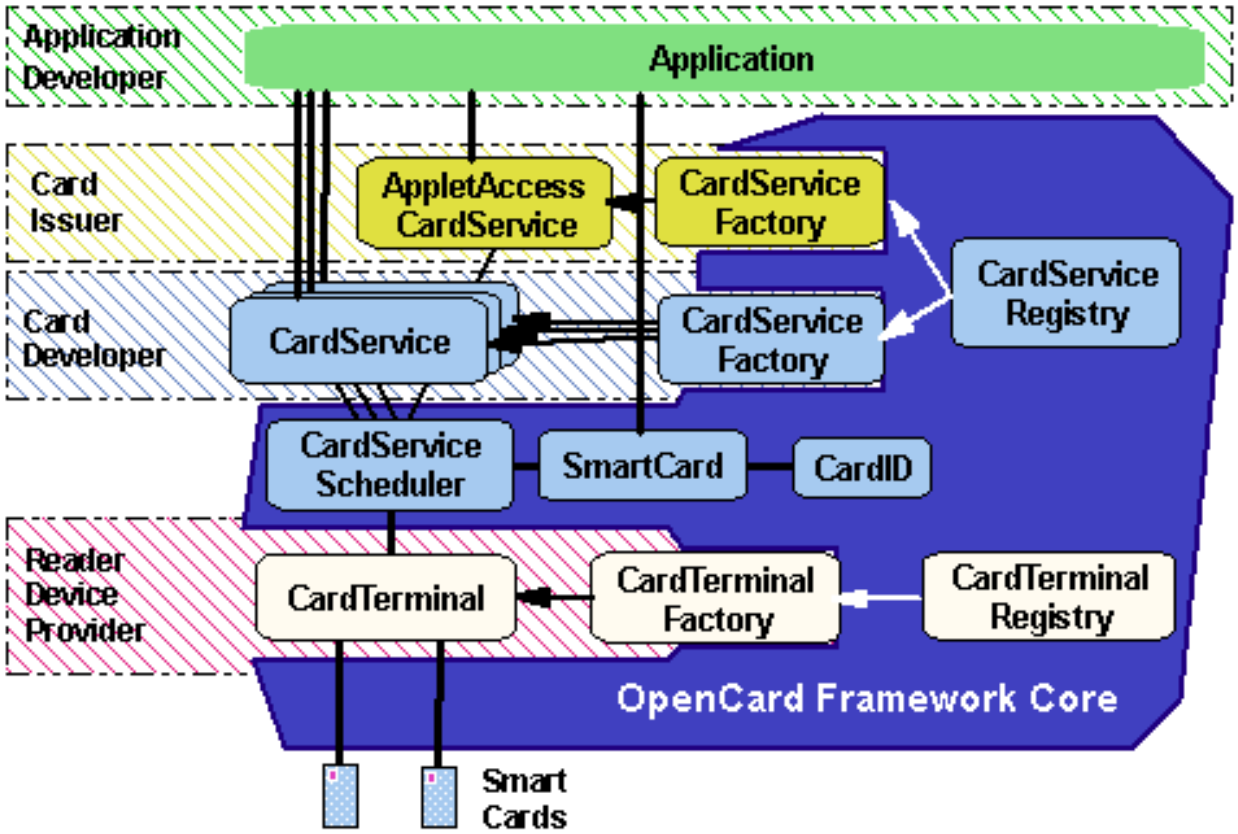



SOURCE: IBUTTON.COM

# OpenCard Framework (OCF)

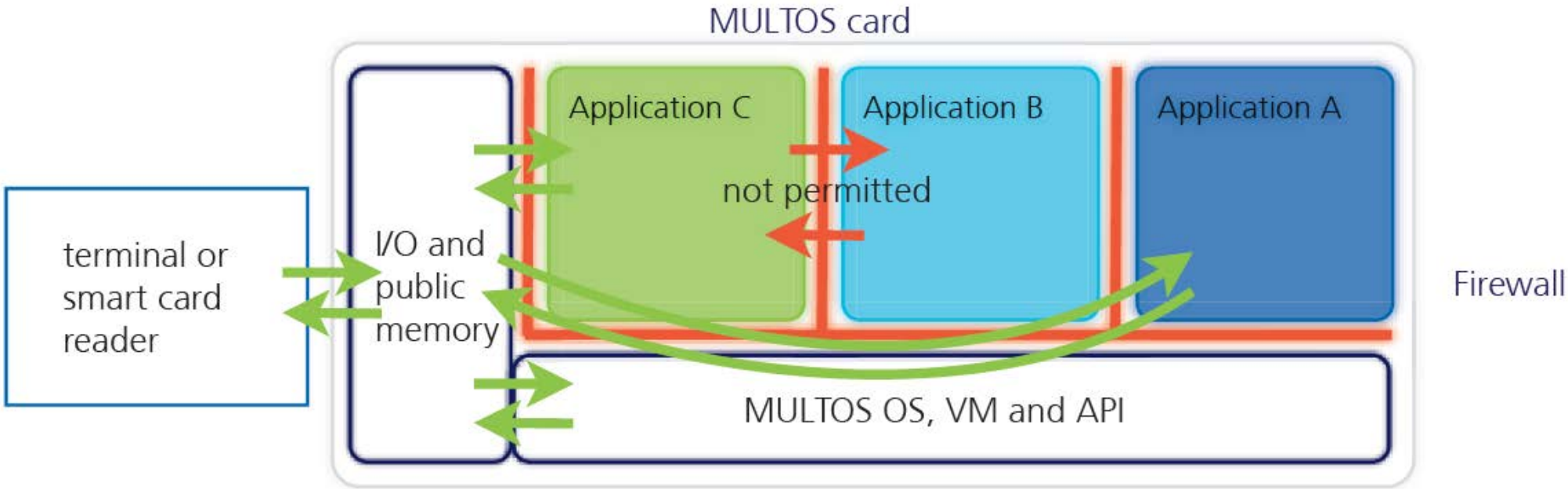
CardService Layer
(TALKS TO CARD)

CardTerminal Layer
(TALKS TO READER)



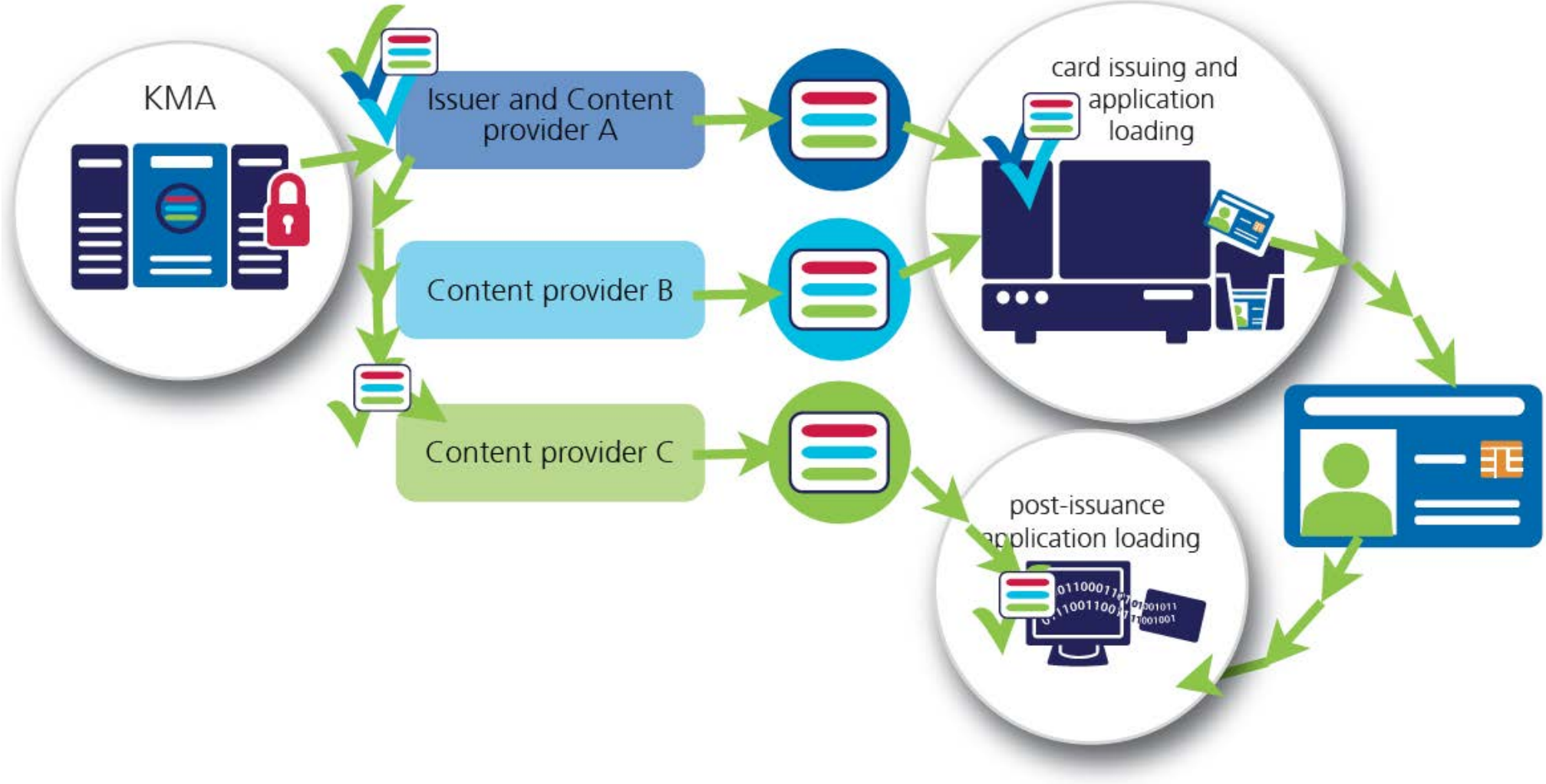

SOURCE: OPENCARD.ORG

# MULTOS Card



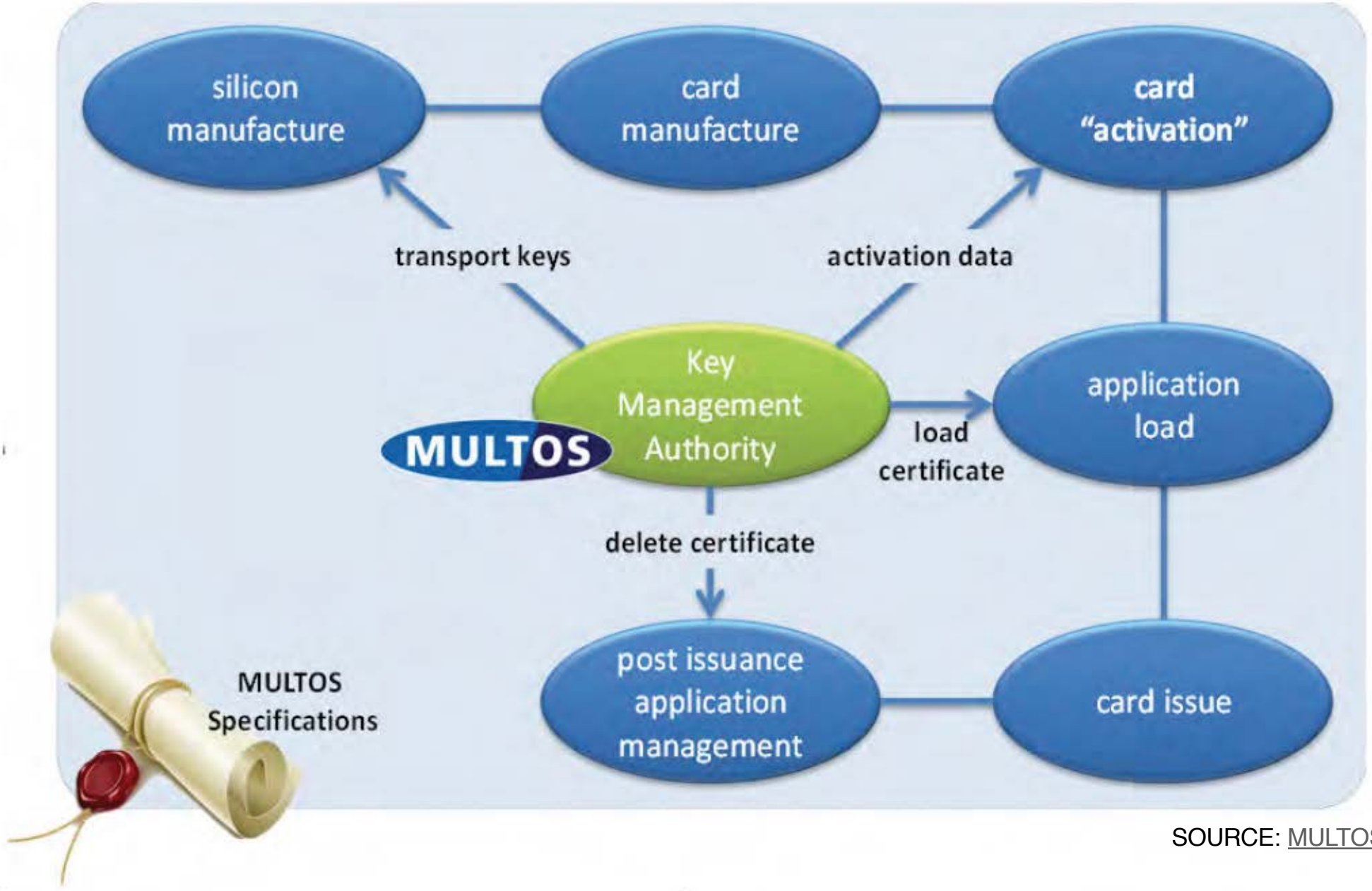

SOURCE: MULTOS

# Hosting Multiple Applications on the same MULTOS Card



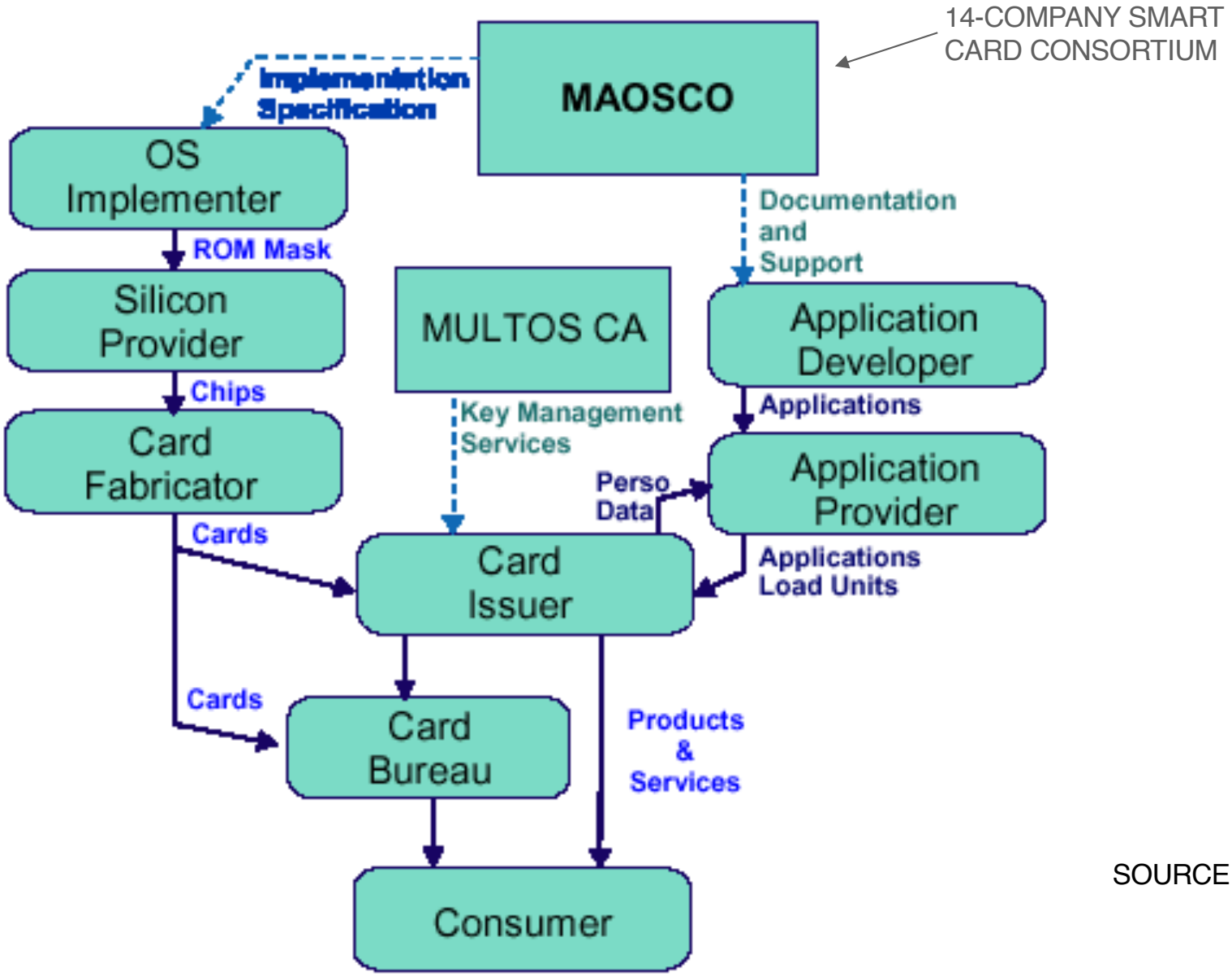

SOURCE: MULTOS

# The MULTOS Scheme




SOURCE: MULTOS

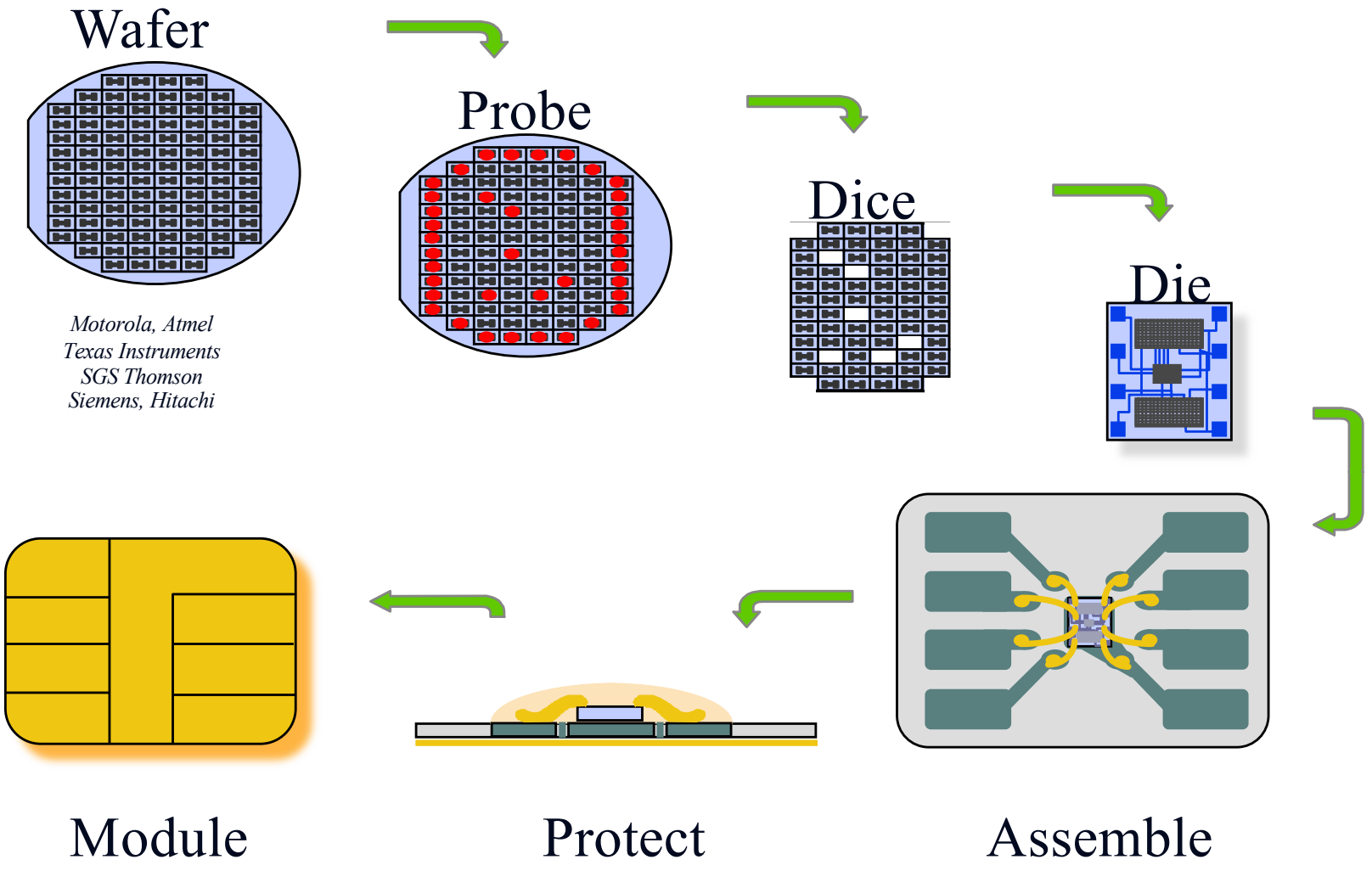
# MULTOS Administration



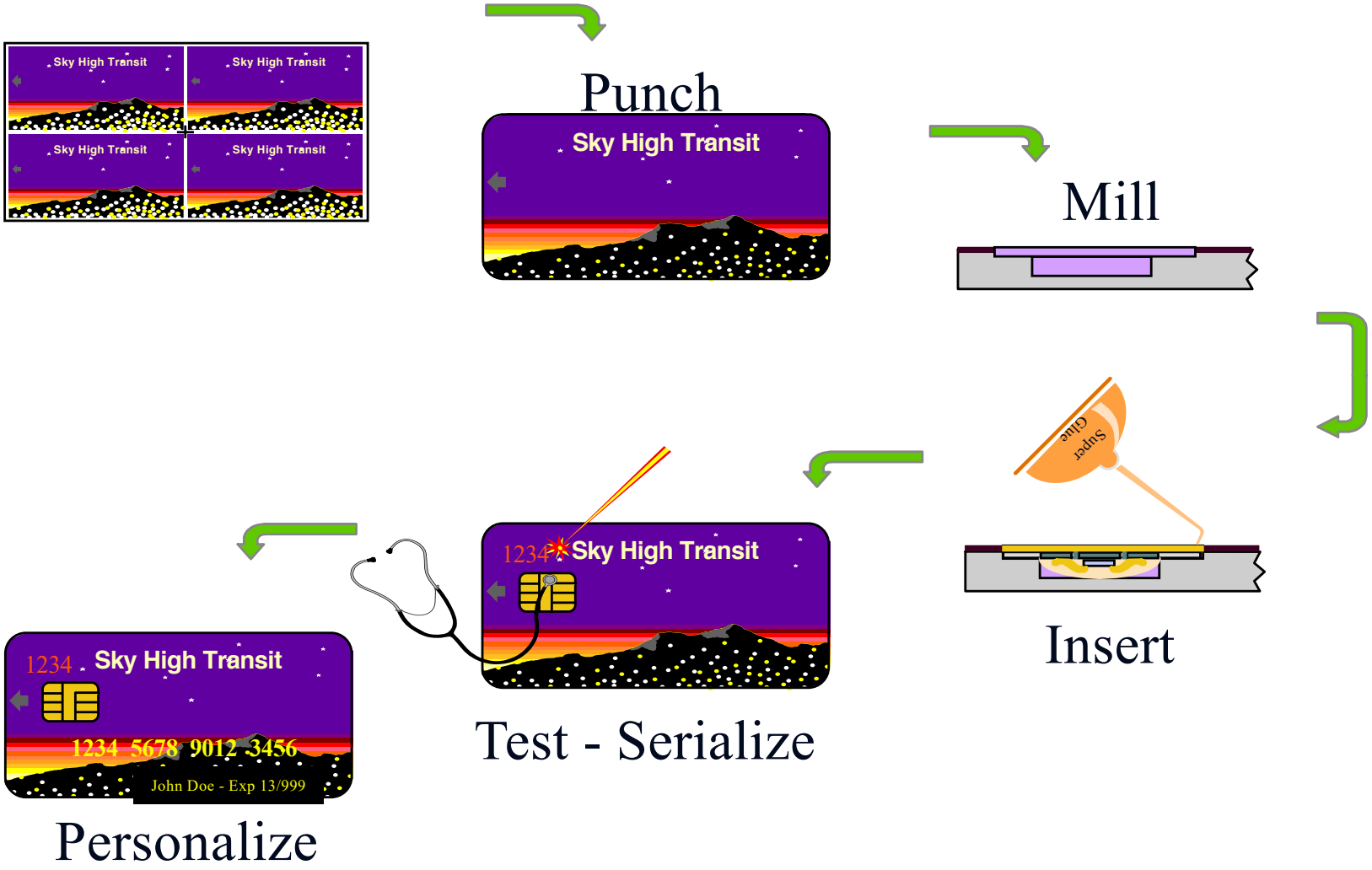

SOURCE: MULTOS

# Card Management
# Pre-Issuance: Manufacturing To Personalization

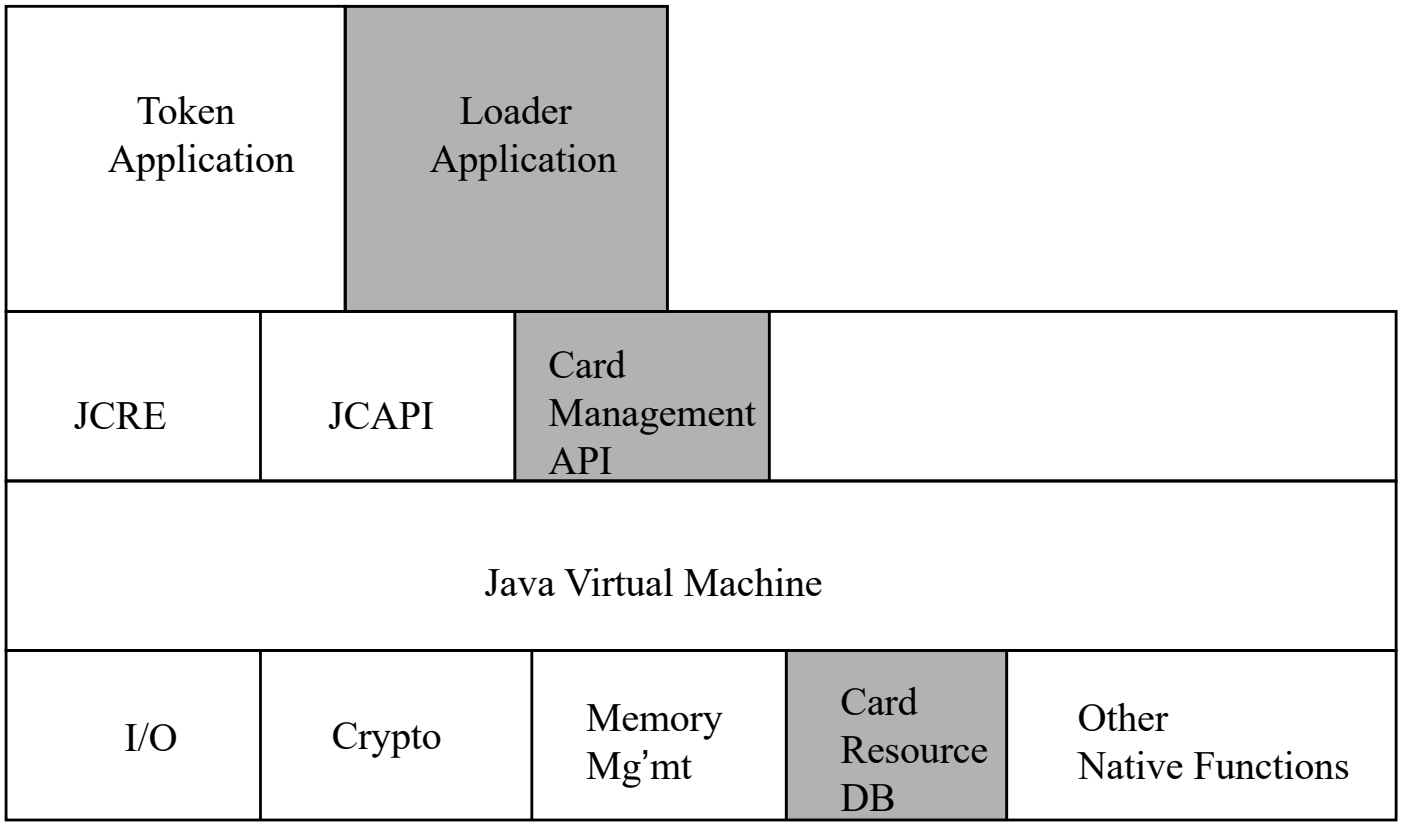
# Module Construction



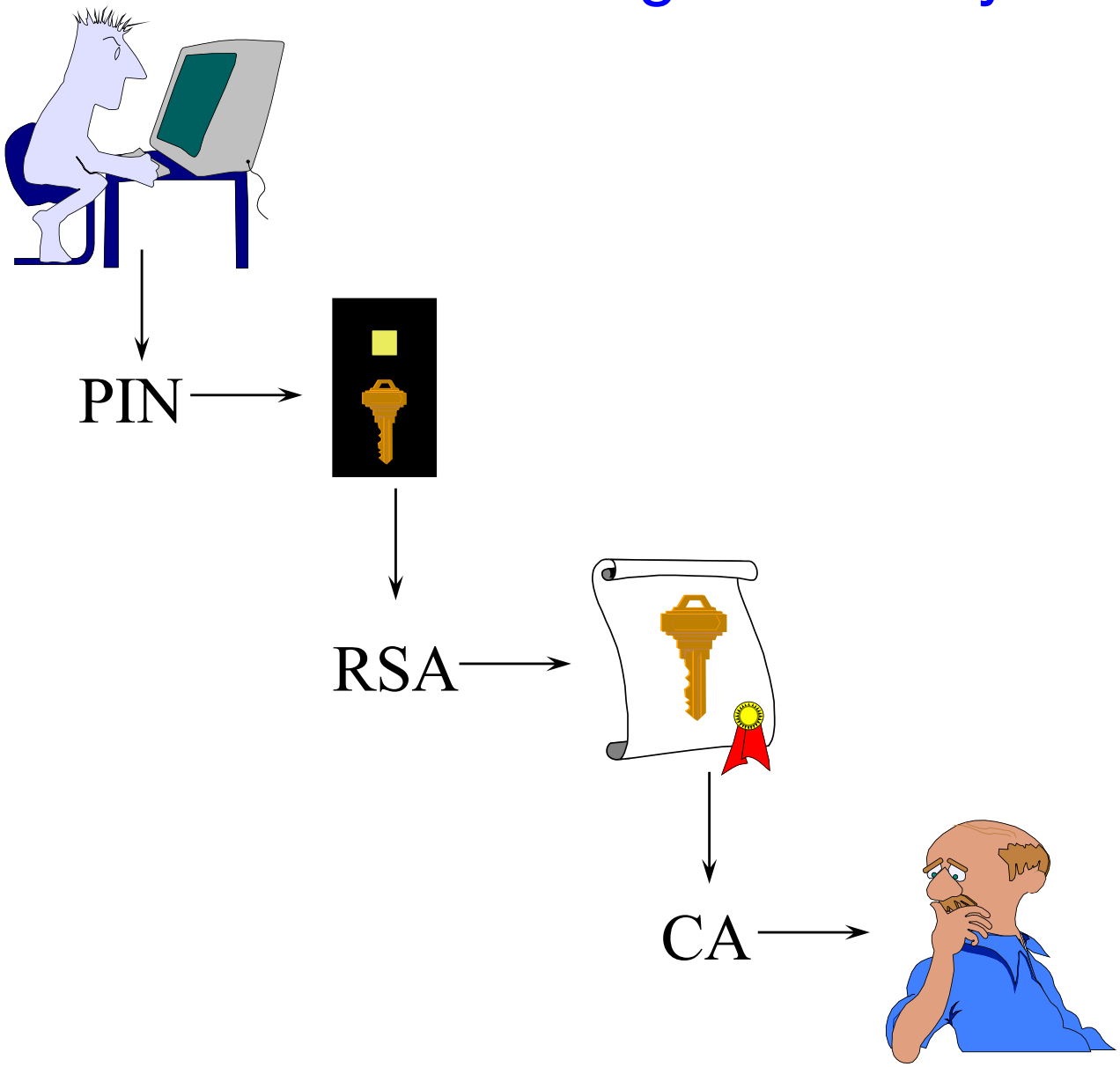
# Card Construction



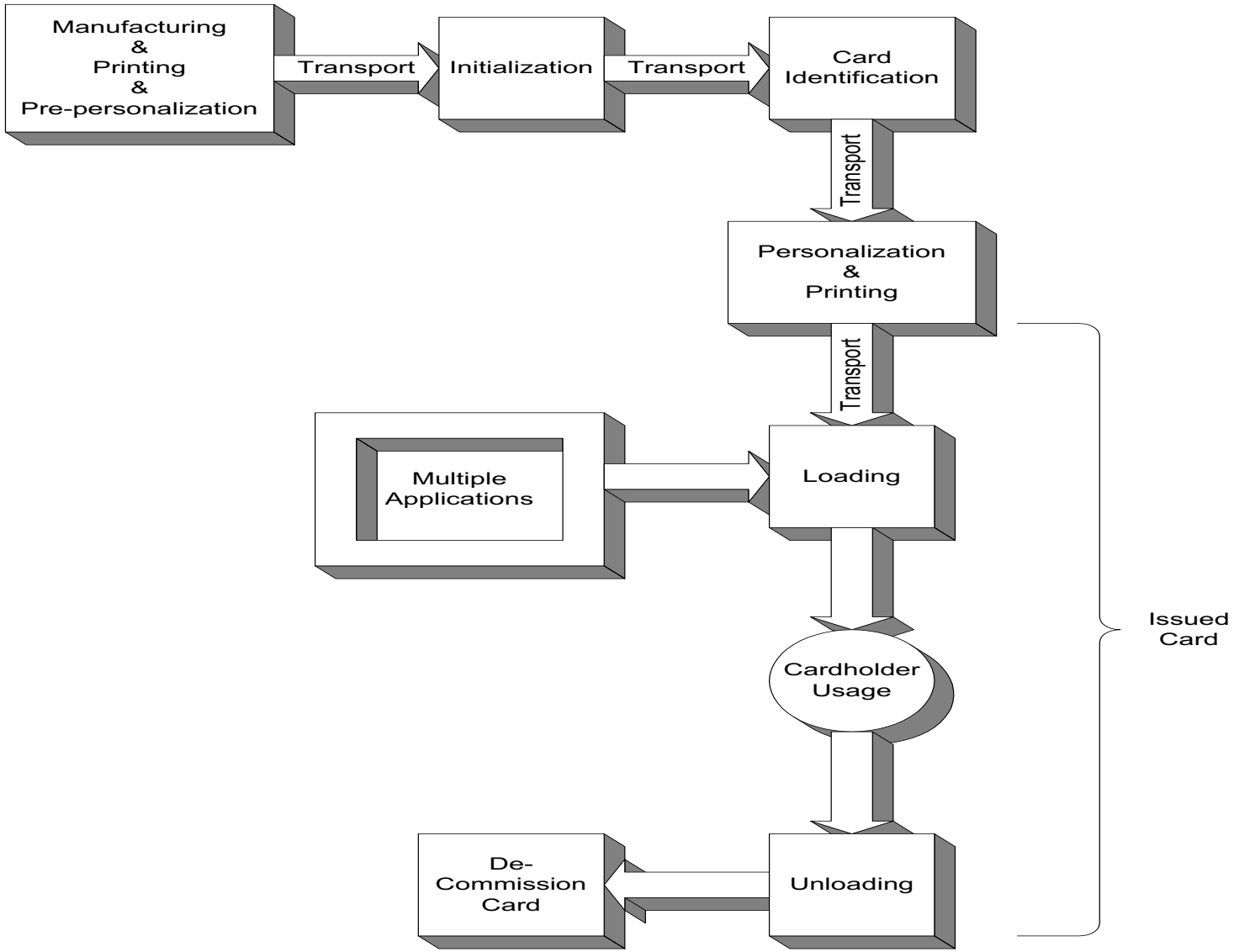
# Example Card



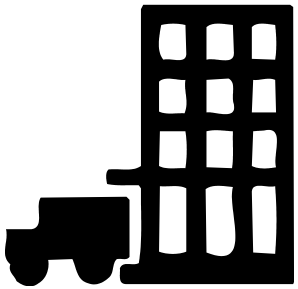
# Digital Identity



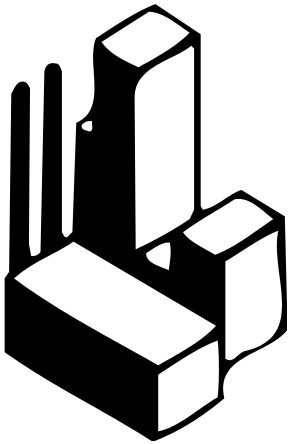
# White Card Card Life Cycle



# Smart Card Lifecycle



Chip Foundry

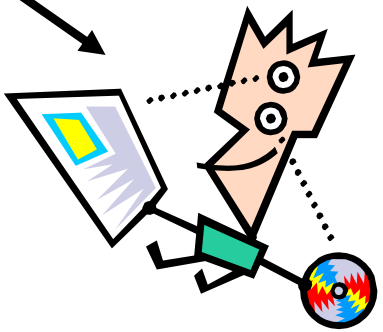


Card Manufacturer

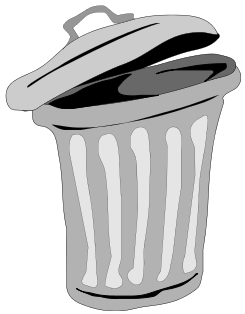
*Pre-personalization*

Issuer

*Personalization*

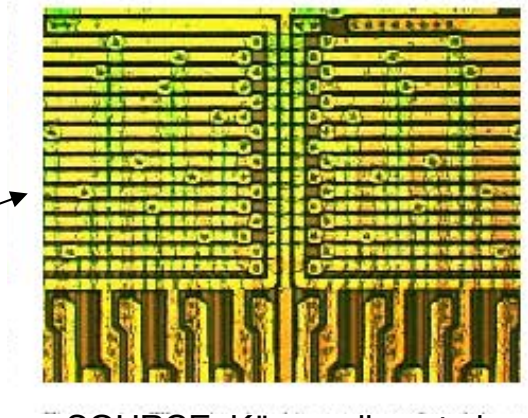


Cardholder

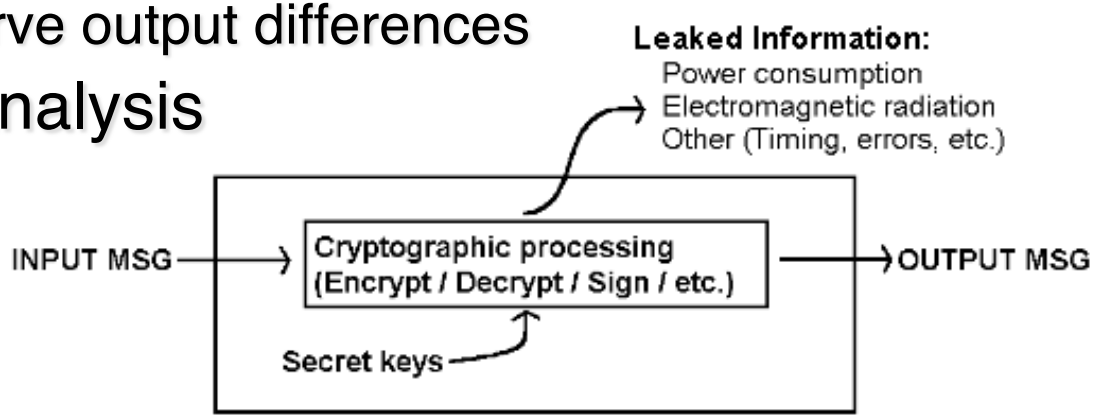


# Smart Card Security

- Observers
- Active defenses
- Attacks:
- Microprobing, microscopy
- Differential fault analysis
  - (Boneh et al. 1997)
  - Induce errors, observe output differences
- Differential power analysis

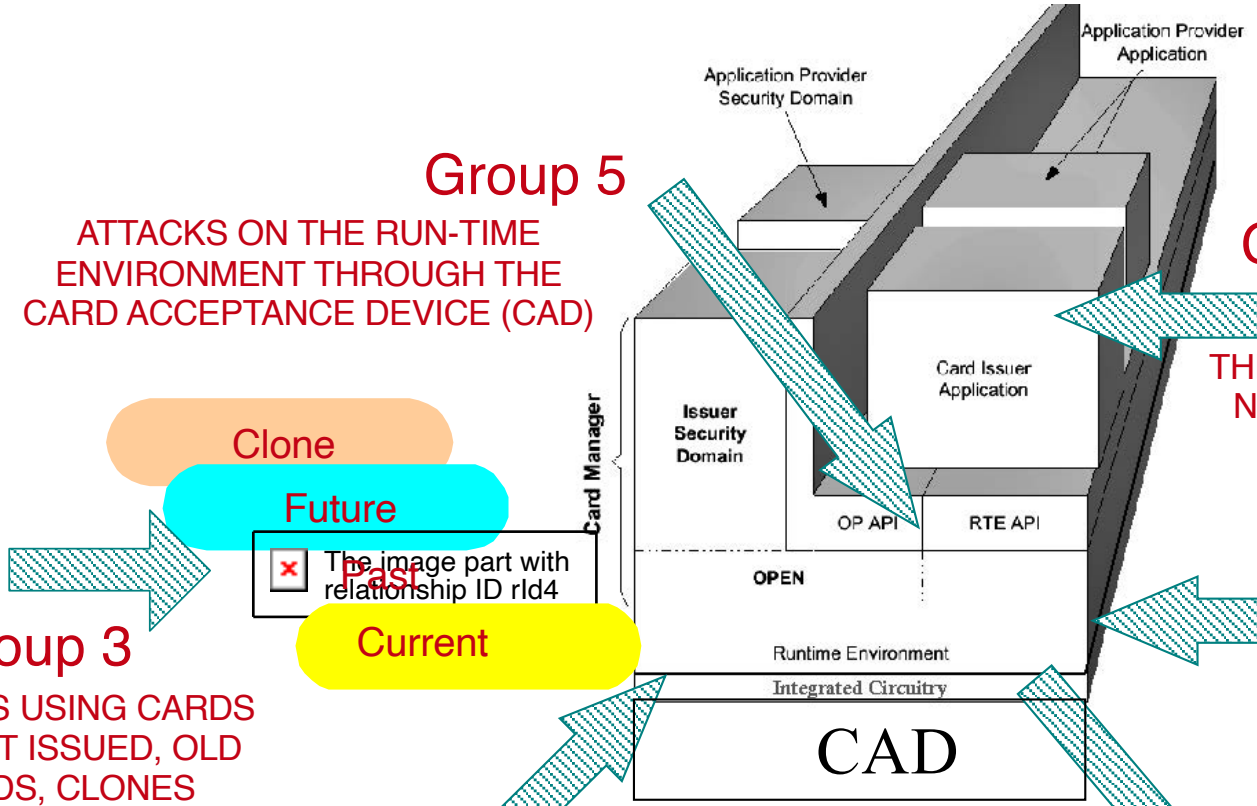


SOURCE: Kömmerling et al.




SOURCE: cryptography.com

# Card Security Threats




## Group 5

ATTACKS ON THE RUN-TIME ENVIRONMENT THROUGH THE CARD ACCEPTANCE DEVICE (CAD)

## Group 6

THREATS FROM CARD APPS AND NEED TO SHARE RESOURCES

## Group 3

ATTACKS USING CARDS NOT YET ISSUED, OLD CARDS, CLONES

## Group 7

THREATS BASED ON RTE IMPLEMENTATION

## Group 1

DIRECT ATTACKS ON CHIP CIRCUITRY

## Group 4

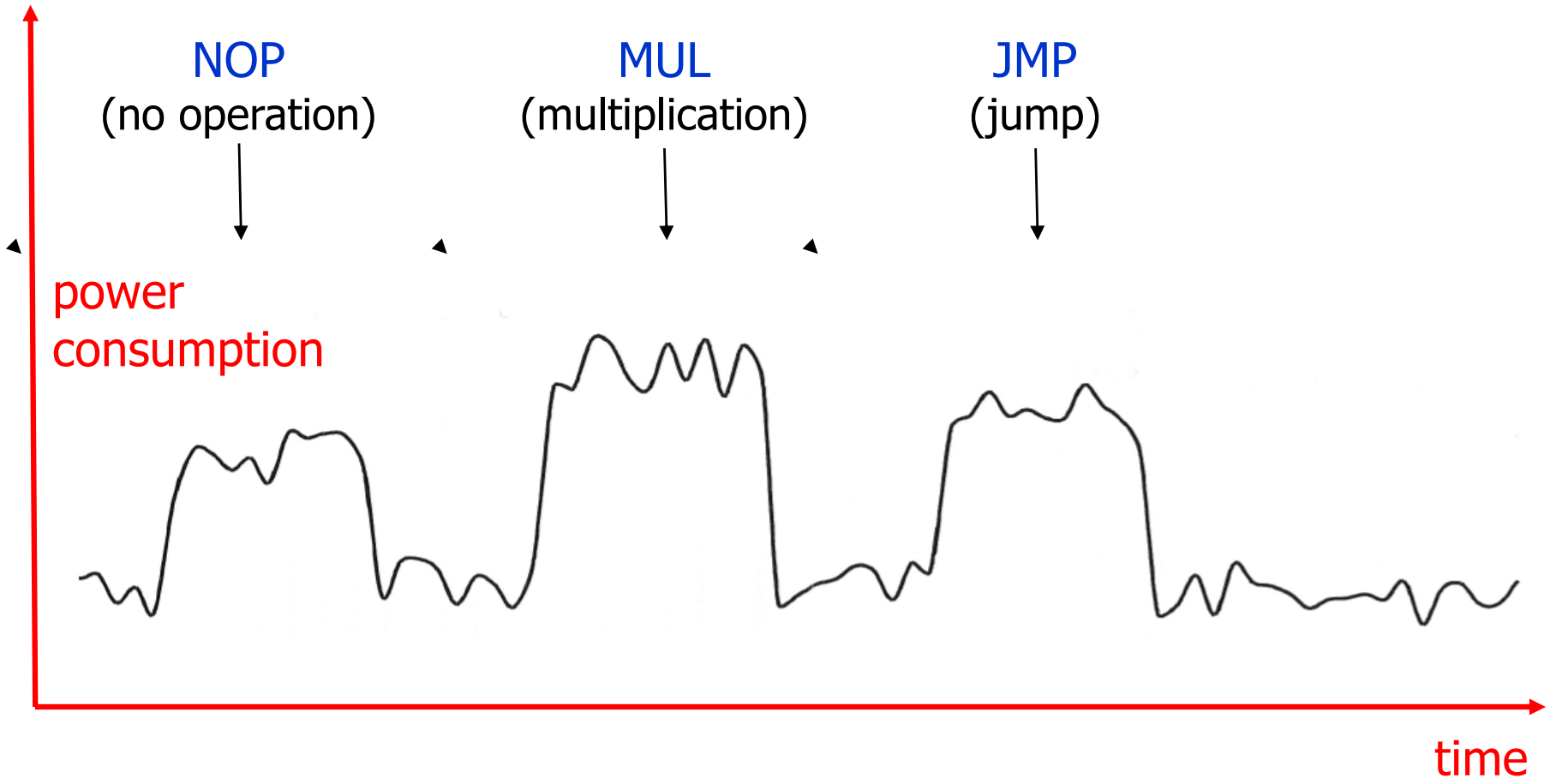
ATTACKS ON CARD'S INTERFACE TO THE OUTSIDE, E.G. PREMATURE REMOVAL

## Group 2

INDIRECT ATTACKS ON CHIP CIRCUITRY

SOURCE: GAMMA

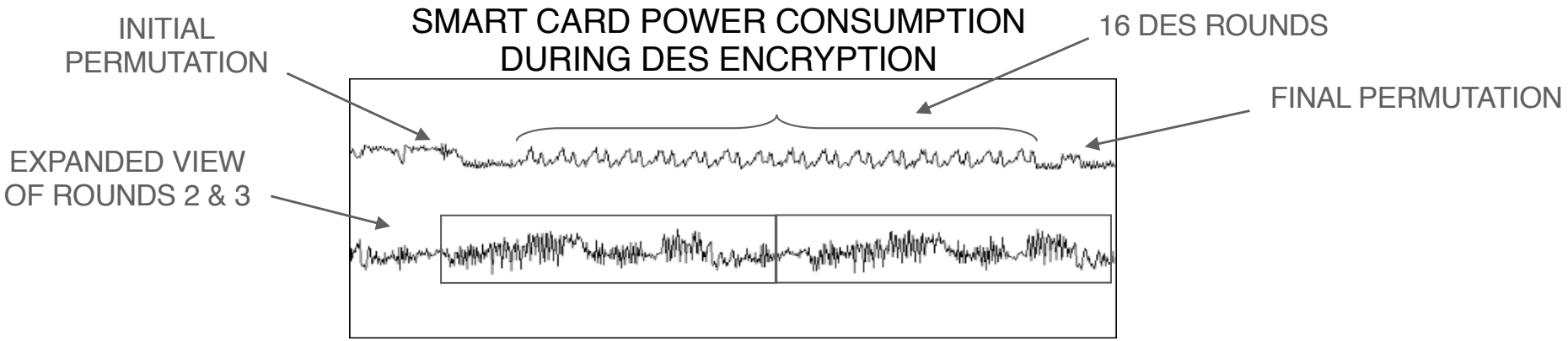
# Power and Timing Analysis




Source: Rankl and Effing, "Handbuch der Chipkarten", 2002

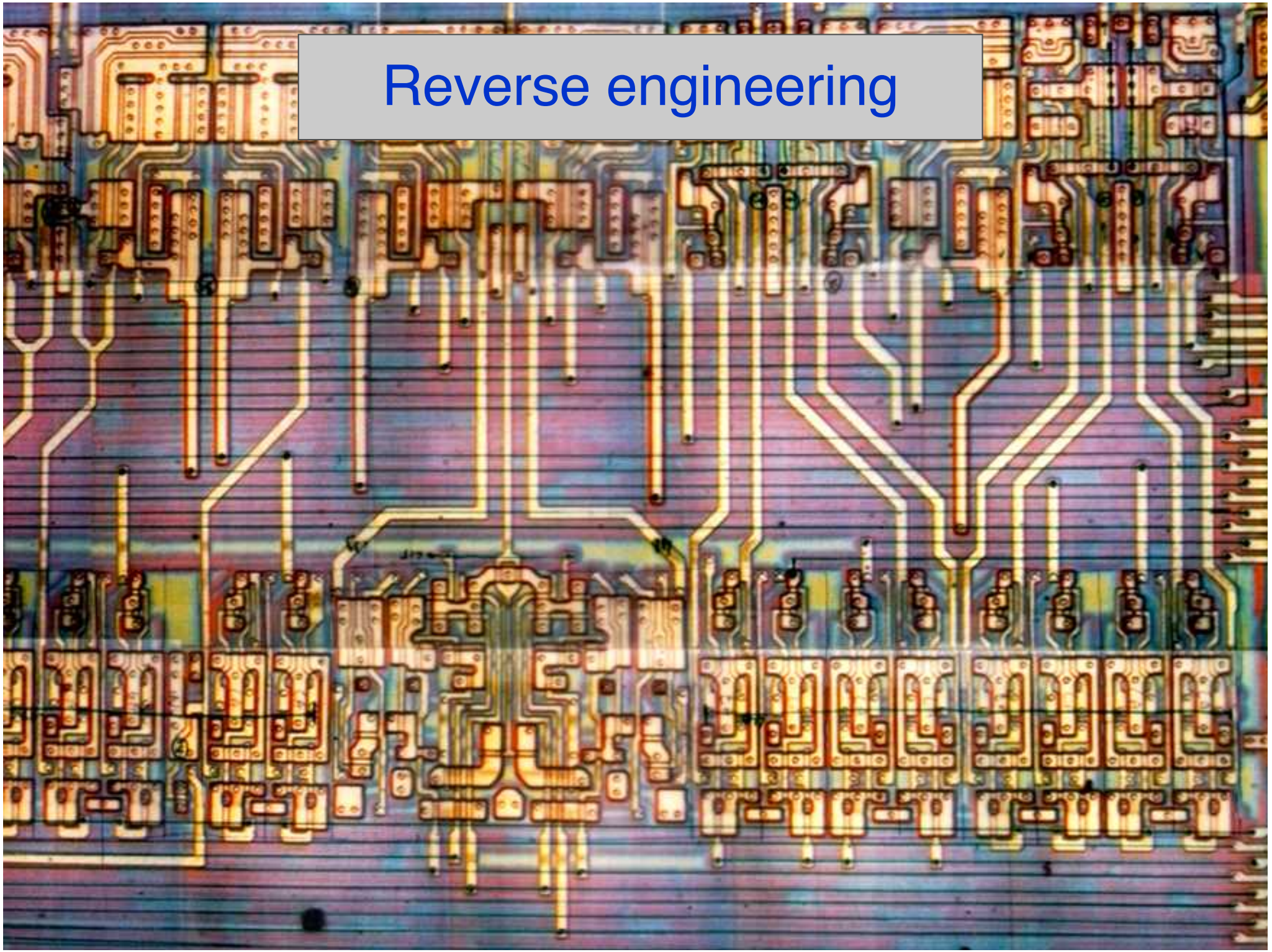
# Differential Power Analysis

- Send different inputs to the Smart Card to learn details of its encryption key
- When a correct key value is tried, the algorithm responds
- Incorrect keys have zero average response

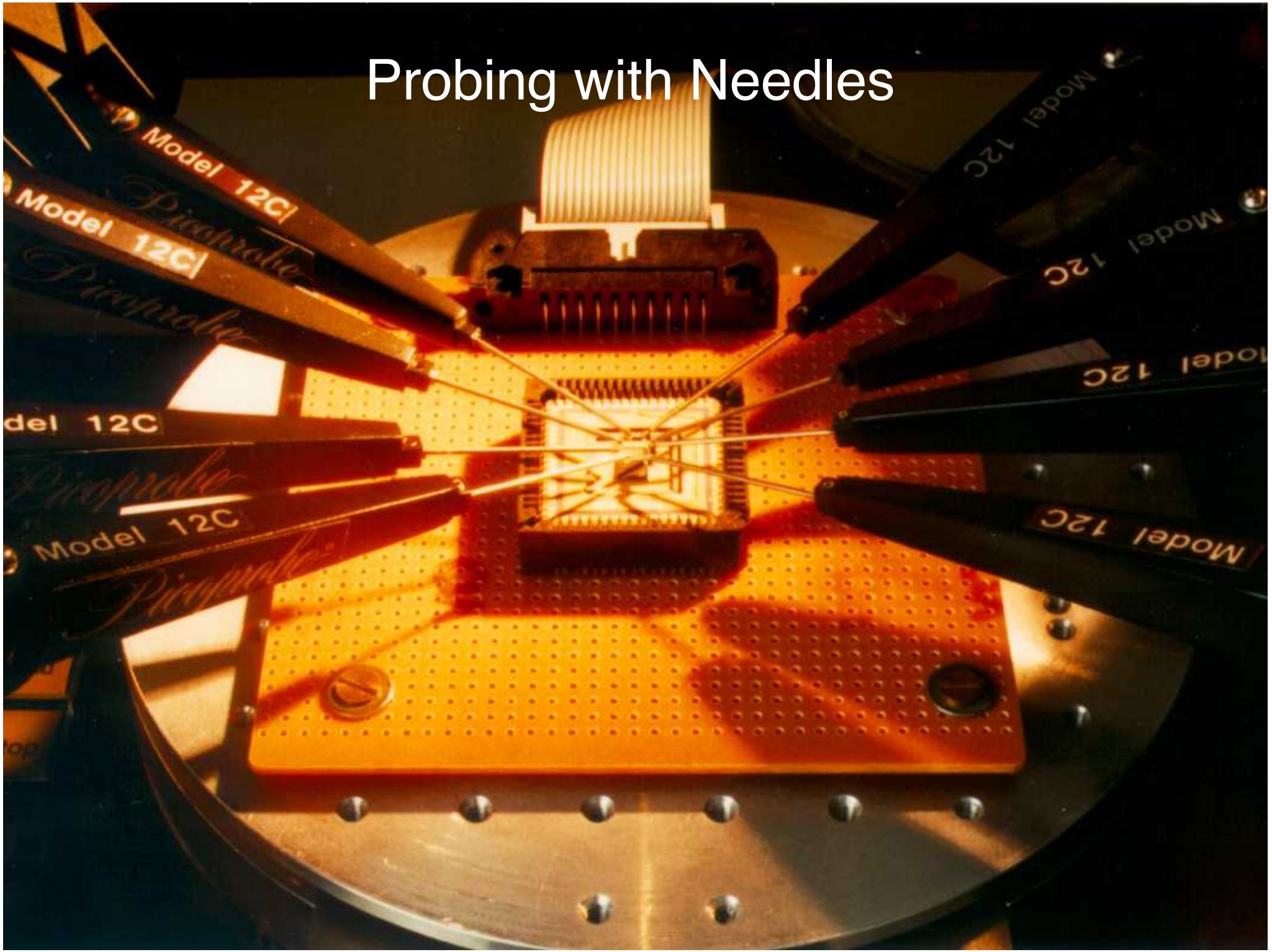



SOURCE: cryptography.com

# Reverse engineering



# Probing with Needles



# Security of the Protocol Messages

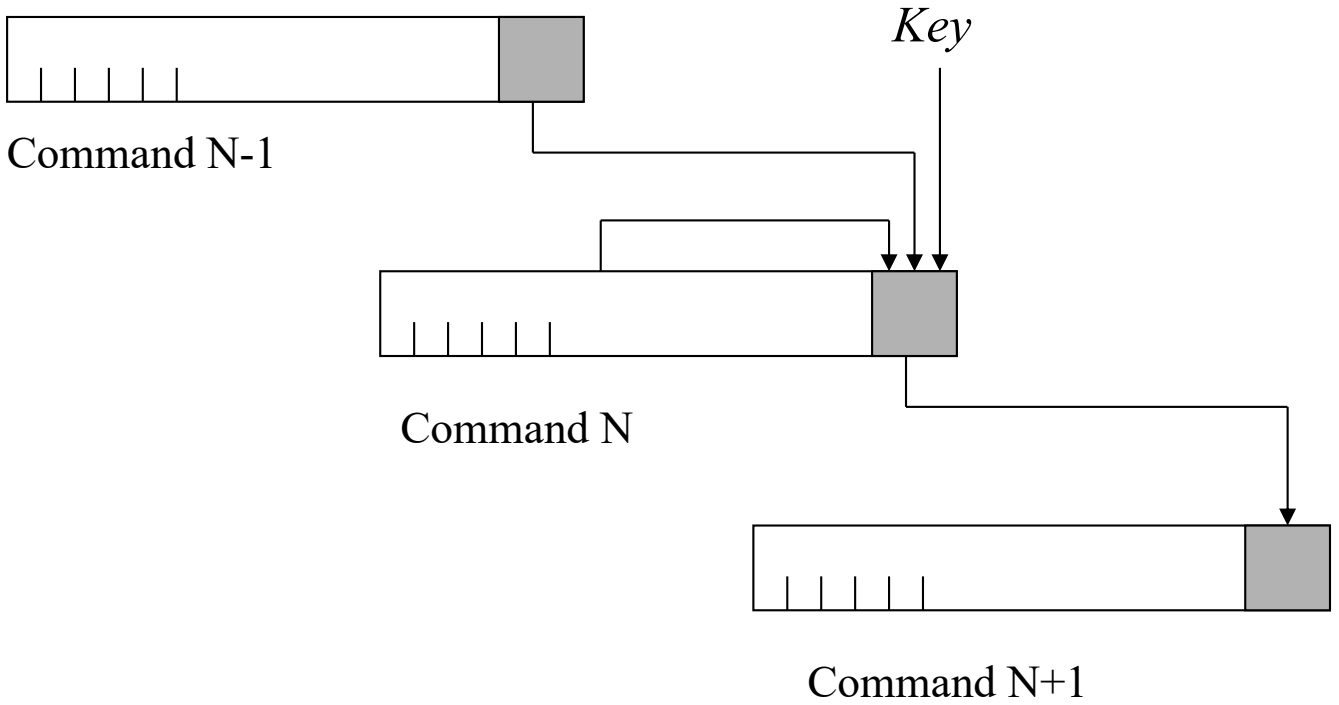
- Secure Messaging
- MACed Commands
- Payment Protocols
- Smart Card Transport

# Secure Messaging

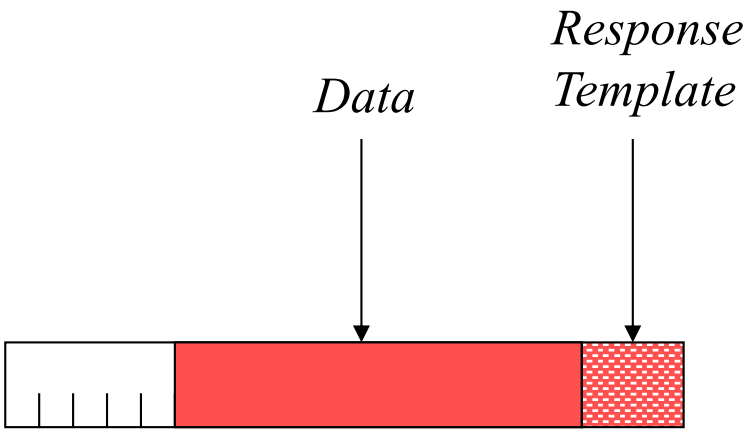
"… to protect (part of) the messages to and from a card by ensuring two basic security functions: data authentication and data confidentiality."

*ISO 7816-4*

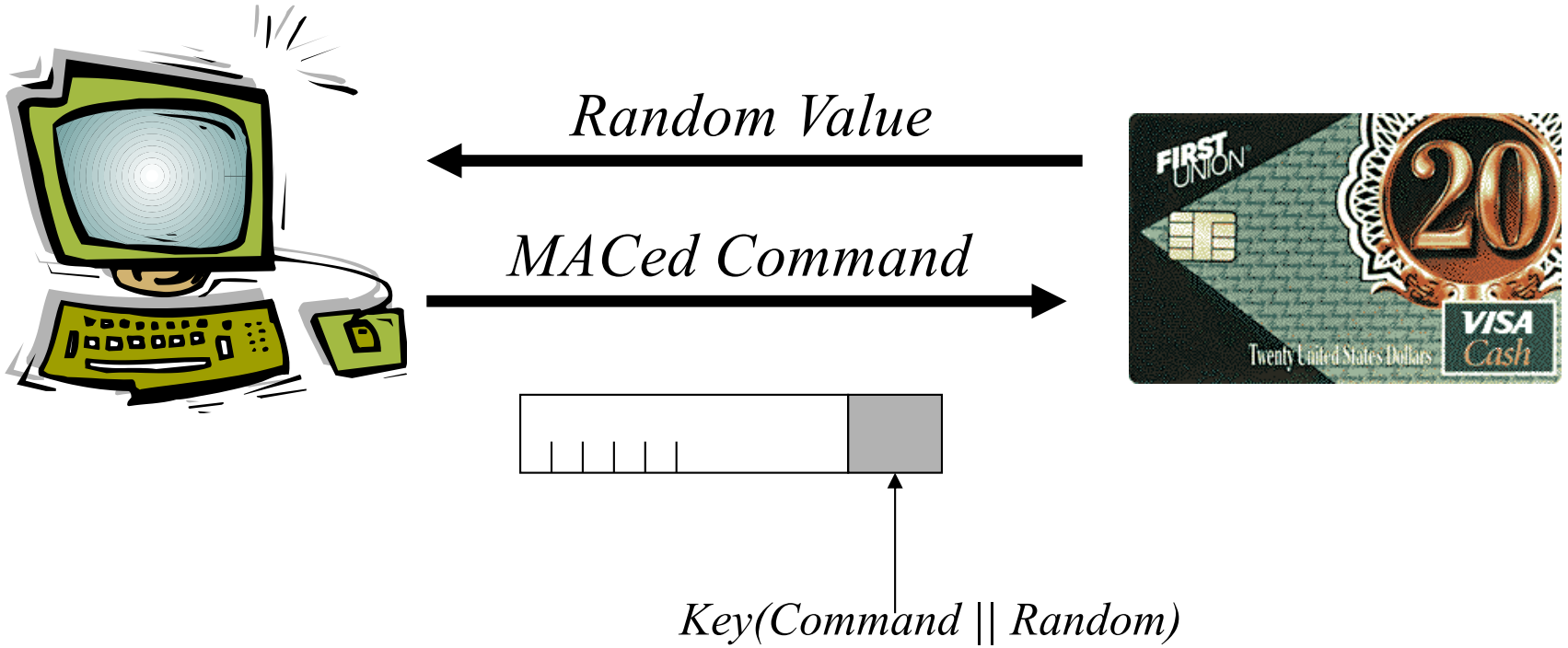
# SM - Authentication



# SM - Confidentiality



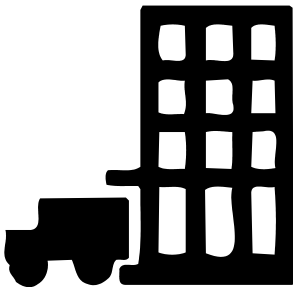

# MACed Commands



# Trudy's Attacks

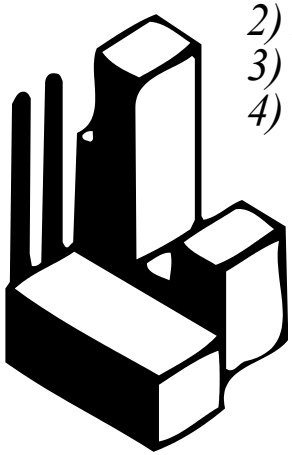
- Man-in-the middle (bucket brigade)
- Replay
- Reflection
- Overrun
- Wastepaper basket
- Rubber hose

# Smart Card Transport



*1) Lock with Foundry Key*

Chip Foundry



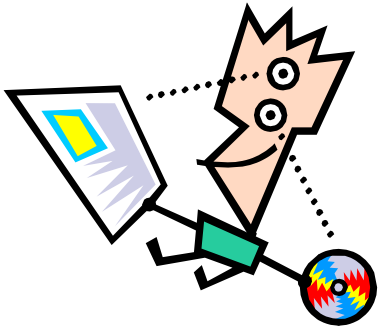
*1) Unlock with Foundry Key*
*2) Add serial number*
*3) Lock with Transport Key*
*4) Deactivate direct memory writing*

Card Manufacturer

*1) Unlock with Transport Key*
*2) Add cardholder identity*
*3) Set unblocking keys and PIN*
*4) Activate special features*

Issuer

*1) Change PIN*



Cardholder

# Smart Cards as Stored Value Facilities (SVF) for Micropayments

- Replacement of cash
  - Cheaper (cash very expensive to handle, stored, require anti-counterfeiting, with risk of loss/theft)
  - Electronic moves easier & faster (cash is not machine-readable, can't carry large amount )
  - Easier to count, audit, verify
- Small transactions, have low value, e.g. < US$1.00
  - Beverages, fast food, Phone calls, tolls, transportation, parking
  - Copying Machine, as well as Online/Internet content/ service
- Must process the transaction at low cost
- Technological savings:
  - Don't verify every transaction
  - No all use Public Key Technologies but pure symmetric encryption
- Float-preserving methods
  - Prepayment
  - Grouping
    - Aggregate purchases (to amortize fixed costs)
    - Provide float to processor
    - Partial anonymity (individual purchases disguised)

# SVF vs. Prepaid Cards for Micropayments

- Prepaid cards
  - Issued by non-banks
  - Represent call on future service
  - Not money since usable only with one seller
- Electronic purse (wallet)
  - Issued by bank
  - Holds representation of real money
  - In form of a smart card (for face-to-face or Internet use)
  - In virtual form (computer file for Internet use)
  - The two forms are converging, e.g. wireless

# Stored Value Facilities (SVF) aka E-Purses/Wallets (Since mid-to-late 90's)


QIANFLEX (CHINA)



AUSTRIAN QUICK


PRISMERA


PEOPLE'S BANK OF CHINA ePURSE


CYBERFLEX JAVA CARD



# Stored-Value SIM Cards



SOURCE: SAMSUNG

# Payment Cards

- Java
- XML, smartX
- PC/SC and OCF OpenCard Framework
- MultOS
- Windows for Smart Cards
- Card-resident app, terminal-resident app
- Card interacts with Web

SOURCE: GEMPLUS

# Payment Cards

- 8-128 Kb
- Data rate 115 Kb/sec
- ISO 7816 compliant
- Visa-certified
- PIN management and verification
- 3DES algorithm for authentication, secure messaging
- Epurse with payment command set (debit, credit, balance, floor limit management)


EMV =
EUROPAY INT'L,
MASTERCARD,
VISA

MPCOS =
MULTI PAYMENT CHIP
OPERATING SYSTEM

SOURCE: GEMPLUS

# SVF (Electronic Purse) Issues

- Loading (charging) the purse with money
- Making a payment (removing money from the card)
- Clearance (getting money into the seller's account)

# Smartcard Payment Protocols: Design Considerations

- **Mutual Authentication**
  - card and terminal must be part of same (closed) system
- **Particular Attention to Man-in-the-Middle Attacks**
  - design for and think in terms of off-line use
  - all authorized parties to the transaction have to be made and kept whole
- **Two-Stages**
  - debit then credit to avoid creating money in case something does go wrong
  - this is another example of built-in disincentives to tampering, experimentation and fraud

# Smart Card Payment Protocol Patents

- US4007355: Data-transfer system (Moreno)
- US4736094: Financial transaction processing system using an integrated circuit card device (Yoshida)
- US5623547: Value transfer system (Jones, Higgins)
- US5637859: Method and apparatus for exchanging information with subscriber cards used in article vending machines (Menoud)
- US5635695: Chip card based payment system having an on-card flag for specifying proper completion of a prior card balance replenishment session (Feiken)


# A Simple Dual-Card Protocol


- Security Access Module (SAM) is the representative of the merchant and the acquiring bank behind him ; SAM is usually installed inside the POS terminal like a SIM card
- Payment Card is the representative of customer and the issuing bank behind him, like our Octopus card
- In many cash and stored value systems, acquiring and issuing entity are the same; i.e. the keeper of the value pool
- Most protocols count on a shared secret between the Payment card and the SAM; i.e. they use symmetric keys
- *Diversified Key*: Payment cards all have different keys and SAM computes a card's key by applying a secret function in the SAM to the card's unique identification number.

# Simple Payment Protocol – Stage I: Debit

*Payment Card to Terminal (e.g. Coke Machine):* Here's a transaction no. and a nonce.

*Terminal to Secure Access Module (SAM = Merchant's card)*: Cardholder wants to spend $1 and here's the transaction number and nonce from the Payment card.

*SAM to Terminal*: OK, here's a debit certificate consisting of the transaction number and nonce plus a debit flag and the amount.

*Terminal to Payment Card*: the cardholder wants to spend $1 and here's the permission from the *SAM* to debit the purse.

*Payment Card to Terminal:* I have checked the debit certificate and it's fine. So I'll debit the purse and remember the amount and the fact that I owe the *SAM (the Merchant)* a credit.

# Simple Payment Protocol – Stage II: Credit

*SAM to Terminal:* Here's my transaction number and a nonce.

*Terminal to Payment Card*: the cardholder wants to spend $1 and here's the transaction number and nonce from the *Merchant (SAM)* .

*Payment Card to Terminal:* I see I have a credit outstanding for that amount so here's a credit certificate consisting of the transaction number and nonce plus a credit flag and the amount. Please deliver this credit to the Merchant (SAM) for me.

*Terminal to SAM:* the cardholder really wants to spend $1 and here's the permission from the payment card to credit your purse.

*SAM to Terminal:* It all checks out fine, so I'll credit the purse of Merchant.
You can now dispense the Coke to the customer.

# Stage I: Debit

- *Cardholder*: Push the “Coke” Button
- *Soda Machine*: Ask Card for identification number, transaction number and nonce; give them to the SAM along with debit amount
- *SAM*: Generate encrypted message containing debit amount, transaction number, challenge and debit flag
- *Card*: Decrypt, check transaction number and nonce, debit cardholder’s purse (remembering the amount), send back “OK” and expect a credit authorization request.

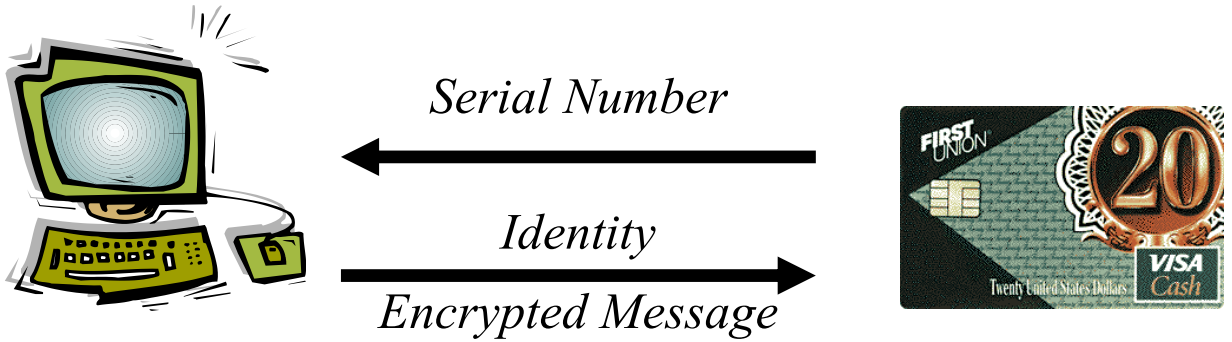
# Stage II: Credit

- *SAM*: Generate transaction number and nonce and send them to the Card with a request to authorize a credit
- *Card*: Return encrypted message containing transaction number, nonce, credit amount and credit flag.
- *SAM*: Check that returned message is OK. If so, credit merchant's purse say "OK" to the Soda Machine.
- *Soda Machine*: Dispense a Coke
- *Cardholder*: Enjoy Coke

# Diversified Keys

- Simple session key protocol for a one-to-many situation like a vending machine
- Unique key for each card without maintaining a list of card keys

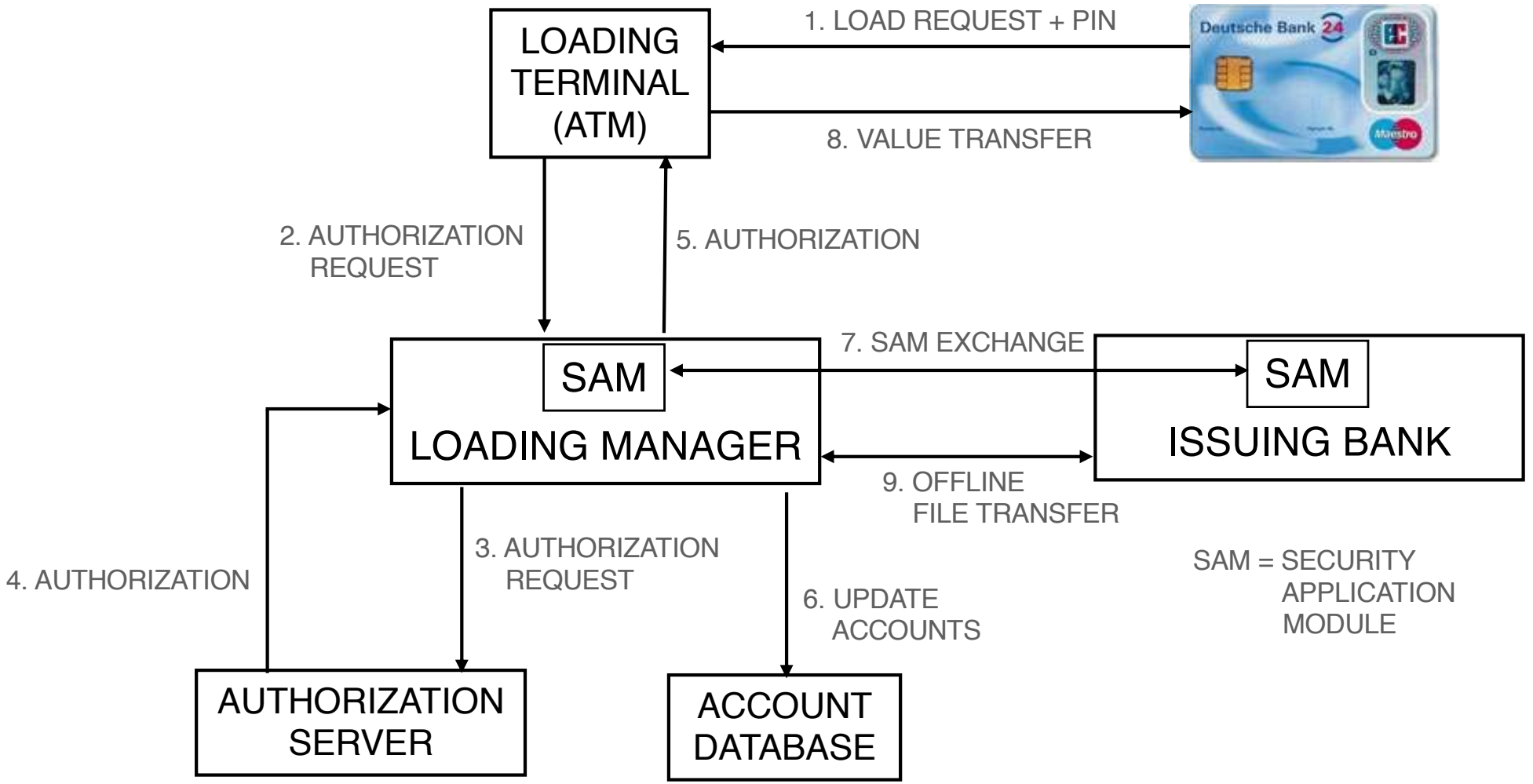
```
Card Key = Crunch(Card Serial Number & Master Key)
```



# GeldKarte (German: “Money Card”)


- Issued by Zentraler Kreditausschuß (Germany) since 1996
- Card contains counters representing money value
  - Max balance 200 EUR ; Average transaction value = 3 Euros.
  - By 2009, 132 million Euros were spent through GeldKarte.
- Card is loaded through a loading terminal
  - Debits customer’s bank account
- Spending at merchant terminal or on Internet
  - Amount deducted from card, added to merchant terminal (card)
  - No real-time authorization
- End-of-day: merchant uploads transactions
- Money credited to merchant account
- Bank fee: 0.3%, minimum USD 0.01
- Many banks now issue cards with Contactless GeldKarte functionalities (branded as Girogo).

# Loading GeldKarte




SOURCE: SHERIF

# GeldKarte Payment

- Customer inserts GeldKarte in slot (at merchant terminal or PCMCIA card)
- Merchant authenticates customer card
- Customer authenticates merchant card

OFFLINE
(NO THIRD PARTY)

- Transfer purchase amount
- Generate electronic receipts

- (Later) Merchant presents receipt to issuing bank to obtain credit to merchant account
- No purse-to-purse transactions

# GeldKarte Card Authentication

- Merchant SAM generates a random number RAND (to prevent replay attack), sends to customer card with request for customer card ID (CID)
- Card sends CID, a generated sequence number SNo, RAND, and H(CID) encrypted with a symmetric secret key $SK_C$ (known to card, not customer)
- No public-key encryption
- Merchant computes $SK_C$ from CID and his own secret key $SK_M$ (known to card, not merchant)
- Merchant can now validate integrity of the card message by computing H(CID)

# GeldKarte Value Exchange

- Customer sends StartPayment message
- Merchant sends MID, merchant's transaction number TNo, SNo, a MAC encrypted with $SK_c$, CID and the value M to be transferred, all encrypted with $SK_c$
- Customer can decrypt this message with $SK_c$ and validate merchant
- Customer checks CID, M and SNo (prevent replay)
- Customer card verifies at least M remaining, subtracts M, increments SNo, records payment data, generates proof of payment and sends to merchant card:

{ M, MID, SNo, TNo, ANo, MAC }

# GeldKarte Value Exchange, cont.

- Merchant verifies payment:
  - compute actual payment amount M' from the proof of payment, compare with M
  - verify MID and TNo
  - increment TNo, increase balance by M
  - notify merchant of success
  - record transaction data with different secret key $K_{ZD}$
- Merchant requests payment from bank (later)
  - sends encrypted proofs of payment to bank
  - TNo prevents more than one credit per transaction

# GeldKarte Clearing

- Uses a “shadow account” (Börsenverechnungskonto) to track the contents of the card
  - When card is loaded, shadow account is credited
  - When money is spent, shadow account is debited
    - online transactions immediately
    - offline transactions later
- If card is lost or damaged, money can be replaced
- Problem: every transaction is recorded, no anonymity
- Solution: “Weisse Karte.” Bought for cash, not connected to any bank account

# GeldKarte Security

- DES (customer), triple DES (merchant) (cipher block chaining or cipher feedback mode)
- 128-bit hashes
- Each card has unique ID, unique symmetric key, PIN stored in “secret zone” and in bank
- Unique transaction numbers

# GeldKarte for Internet Payment and beyond


"Caroline" Trusted Wallet Device

GeldKarte Reader USB or Infrared Connection to PC

CASHMOUSE

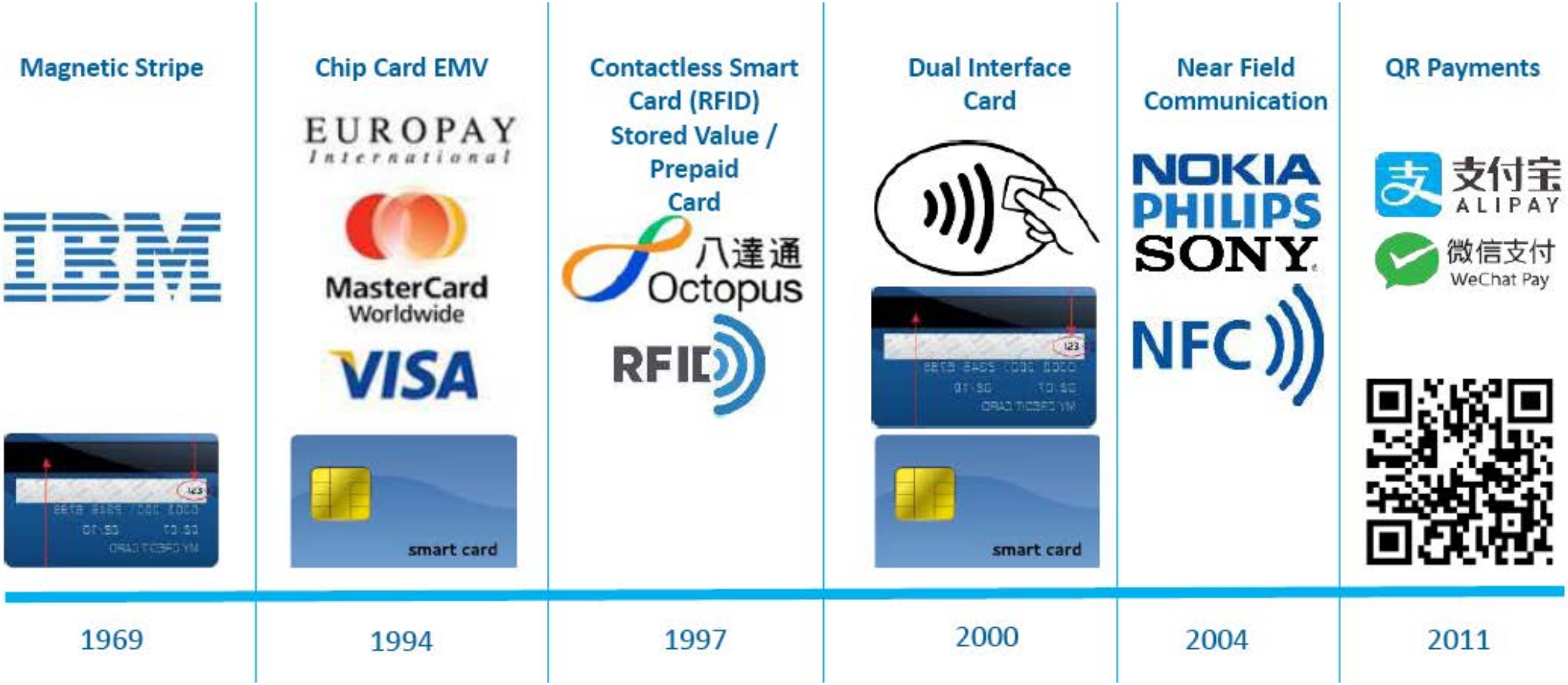
- Contactless Card supporting GeldKarte has become available ; branded as Girogo, as a "Prepaid" function supported by the Girocard (Debit-card)

girocard

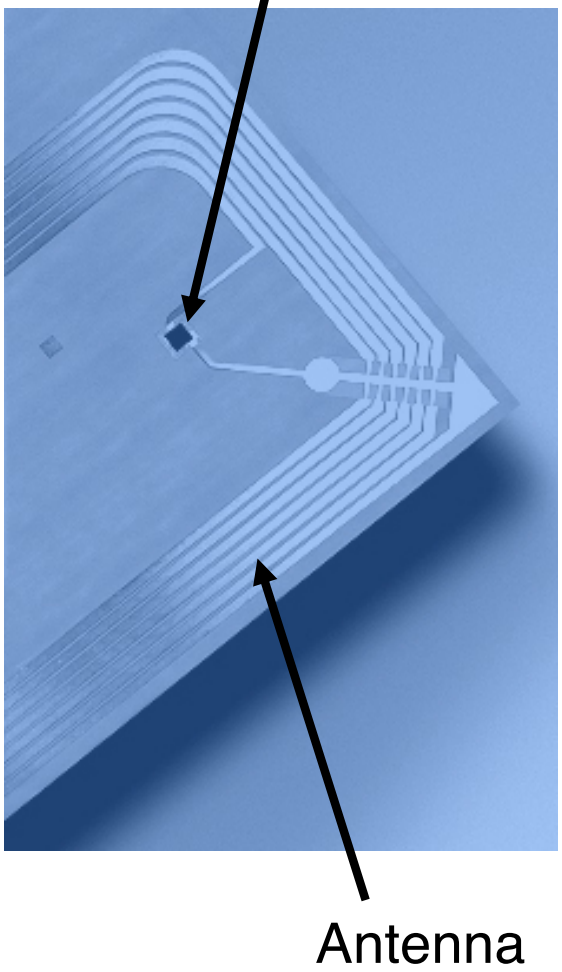
# Other Smartcard-based Payment Systems/ Protocols

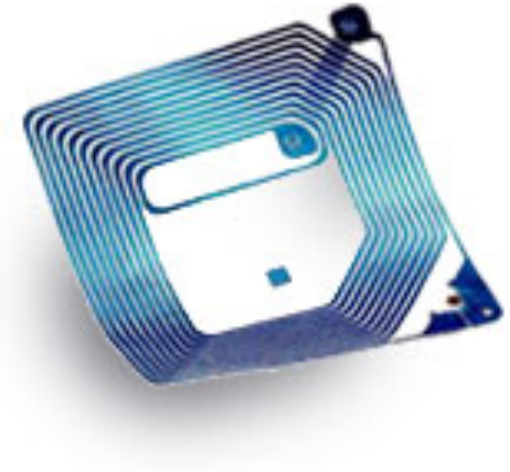
- **Cash vs. Stored Value vs. Credit/Debit**
- **Danmont and Mondex**
  - the original smart card cash protocols
  - Danmont is accounted, Mondex is anonymous
- **VisaCash, Proton, GeldKarte, …**
  - Danmont led to many follow-on systems
- **EMV for debit/credit**
  - EMV was first attempt at describing a multi-application card
- **CEPS Protocol**

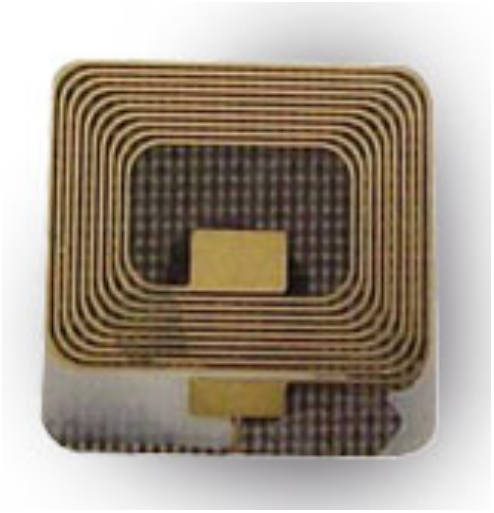
# Payment Media Evolution



# RFID Tags



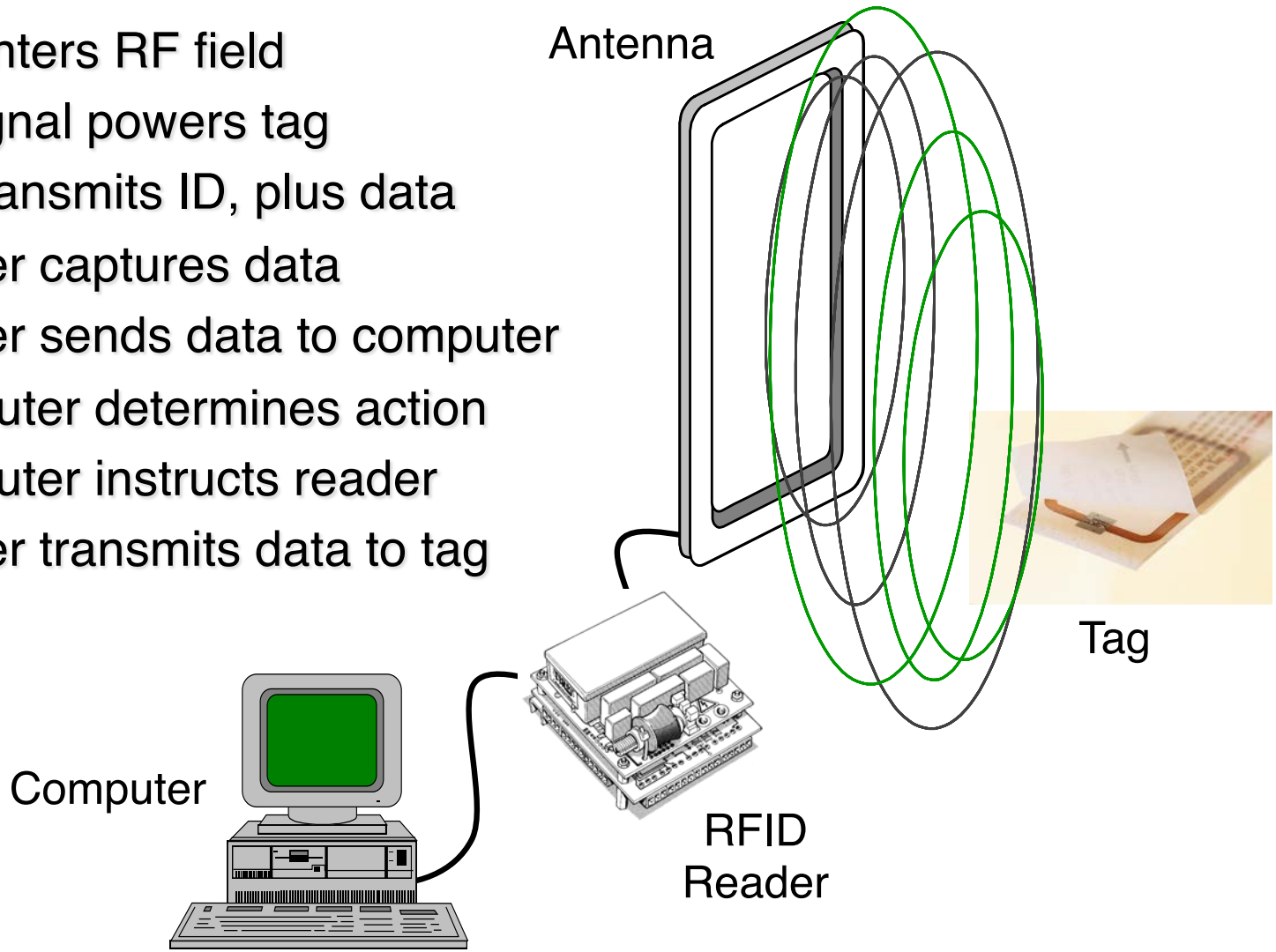





32mm and 23mm
capsule transponder

# How RFID Works

- Tag enters RF field
- RF signal powers tag
- Tag transmits ID, plus data
- Reader captures data
- Reader sends data to computer
- Computer determines action
- Computer instructs reader
- Reader transmits data to tag




SOURCE: PHILIPS

# Euro Banknotes

- In 2001, European Central Bank has announced planned to implant RFID tags in banknotes by 2005


- Uses
  - Anti-counterfeiting
  - Tracking money flows

- BUT the plan NEVER materialize !

# Typical spec for Contactless and RFID tags (circa 2005)

| Class | Frequency | Speed | Storage | Apps | Memory |
|---|---|---|---|---|---|
| Proprietary | 125-134 kHz | 4kbps | 8-2kbits | Access, Inventory | ROM, EPROM |
| Proprietary (EPC) | 866-956 MHz | 20-100kbps | 512bits | Tolling, Inventory | ROM, EPROM |
| ISO18000 | 2.45GHz | 40kbps | 512bits | Tolling, Inventory | ROM, EPROM |
| ISO 14443 | 13.56Mhz | 106, 212, 424, 848kbps | 64bytes – 64kbytes | Access, Payment | ROM, RAM EEPROM, FRAM |
| ISO 15693 | 13.56Mhz | 26Kbps | 1kbit, 2kbit, 16kbit | Access, Inventory | ROM, RAM EEPROM, FRAM |

SOURCE:
https://www.secureidnews.com/news-item/understanding-the-different-memory-types-used-in-contactless-smart-cards-and-rfid-tokens/

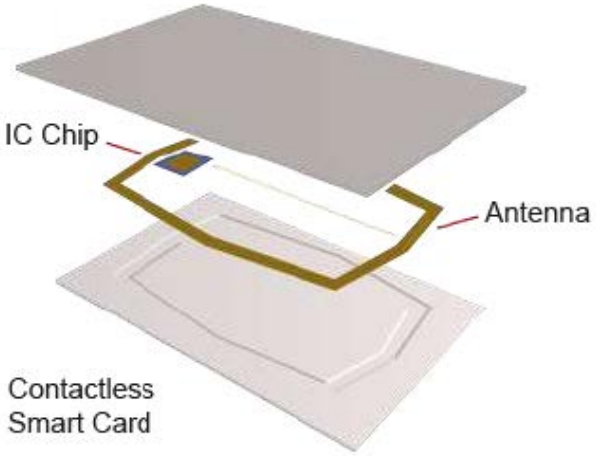
# Contactless Smart Cards


- Communicates by radio
- Power supplied by reader
  - Low Frequency (LF) Proximity (low-cost) Card: 125-134 kHz ; typical usage for Door Access
  - High Frequency (HF) at 13.56MHz (ISO 14443/ 15693 standards) for ID credentials, Passports, Bankcards (ISO 14443 standards)
  - Effective range: 10 cm, signals encrypted
  - Ultra High Frequency (UHF) operates at 433 to 953 MHz has longer range upto 30 feet, 10-15 feet for good accurarcy ; commonly used in RFID tags for logistics applications and asset tracking
  - Data rate:  from ~100 Kbit/sec upto 848 KByte/sec (NXP Mifare)
  - Read 2.5 ms, write 9 ms
  - 8 Kb EEPROM, unlimited read, 100,000 writes
  - Lifespan: 4-5 years vs. ~ 2 years of contact-card (data retention 10 years)
  - Two-way authentication, nonces, secret keys
  - Anticollision mechanism for multiple cards
  - Unique card serial number

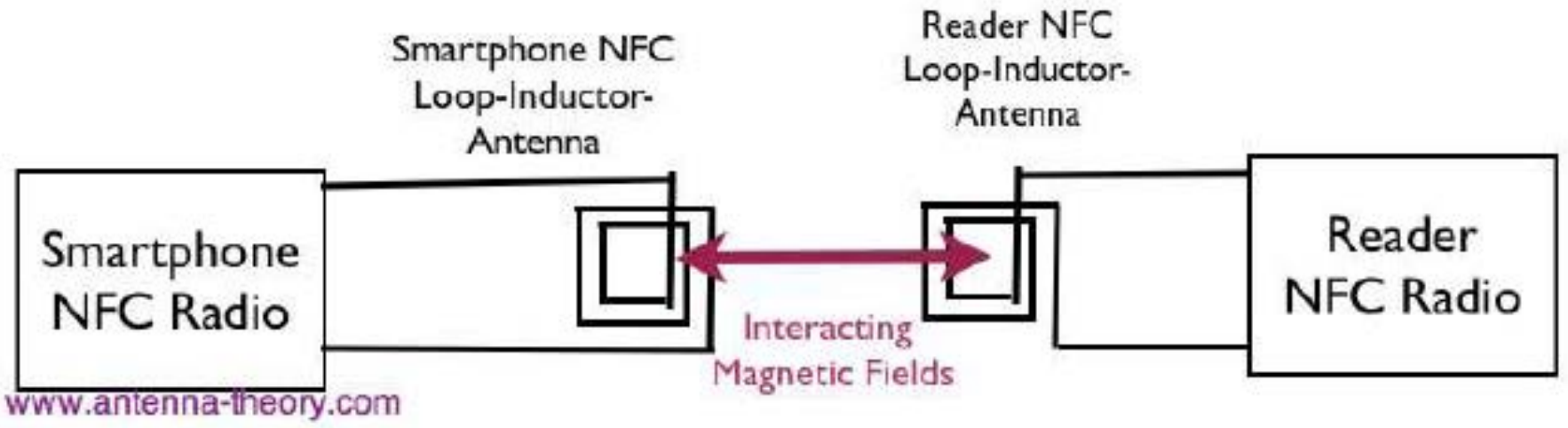
SOURCE: GEMPLUS ; https://www.secureidnews.com/news-item/tech-101-contactless-smart-cards/

# Contactless Smart Cards Operating Sequence

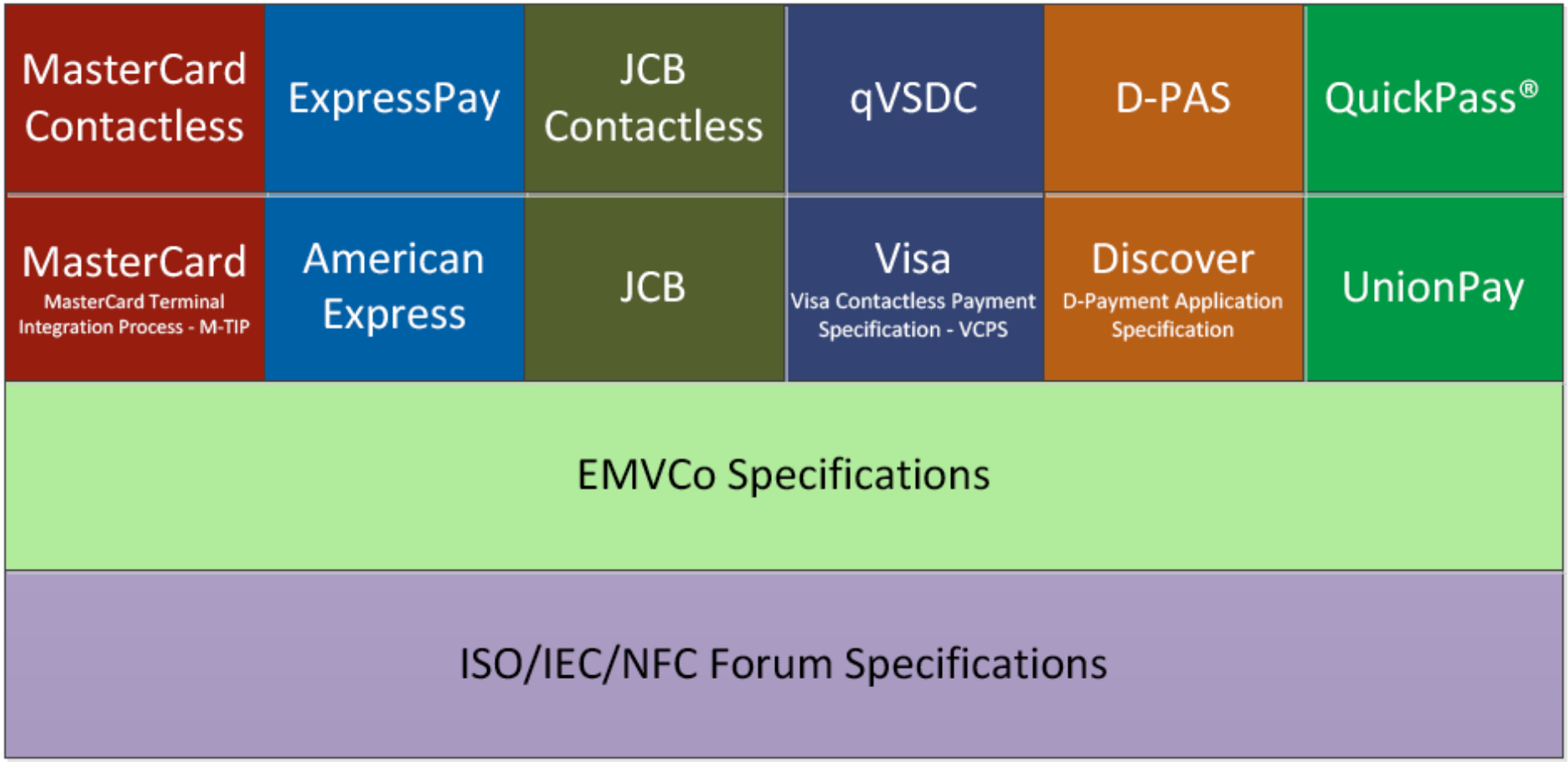
- Contactless smart card contains an antenna within the plastic body of the card
- When the card is brought into the EM field of the reader, the chip in the card is Powered ON
- Once the chip is powered on, a wireless protocol is initiated and established between the card and the reader for data transfer
- Two-step sequence:
  - Energy transfer to the card for powering the IC
  - Clock Signal Transfer
  - Data Transfer to the contactless smart card Card
  - Data Transfer from the contactless smart card

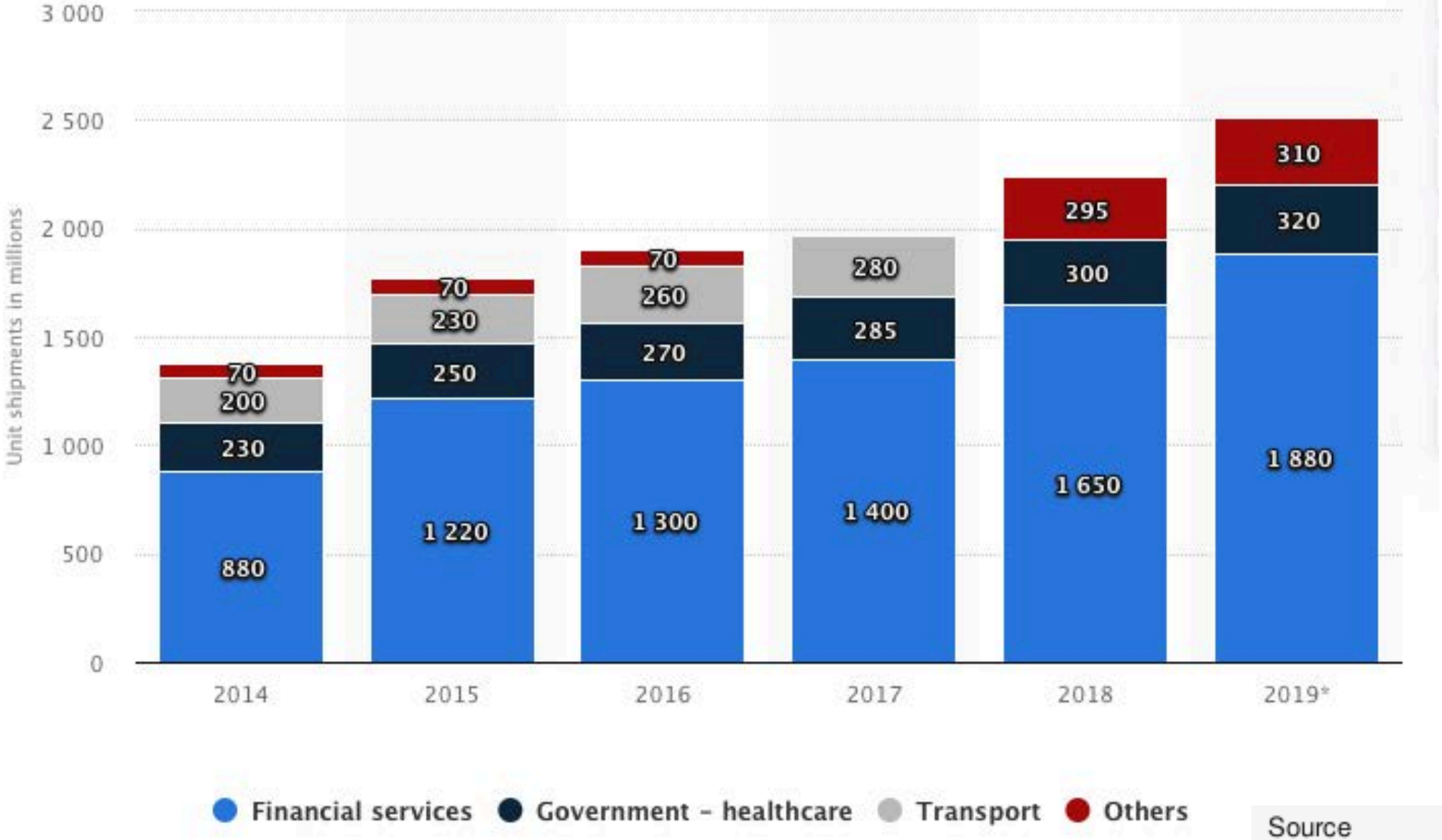
# Near Field Communications (NFC)



# Relationship among EMVCo and Contactless Payment Specifications



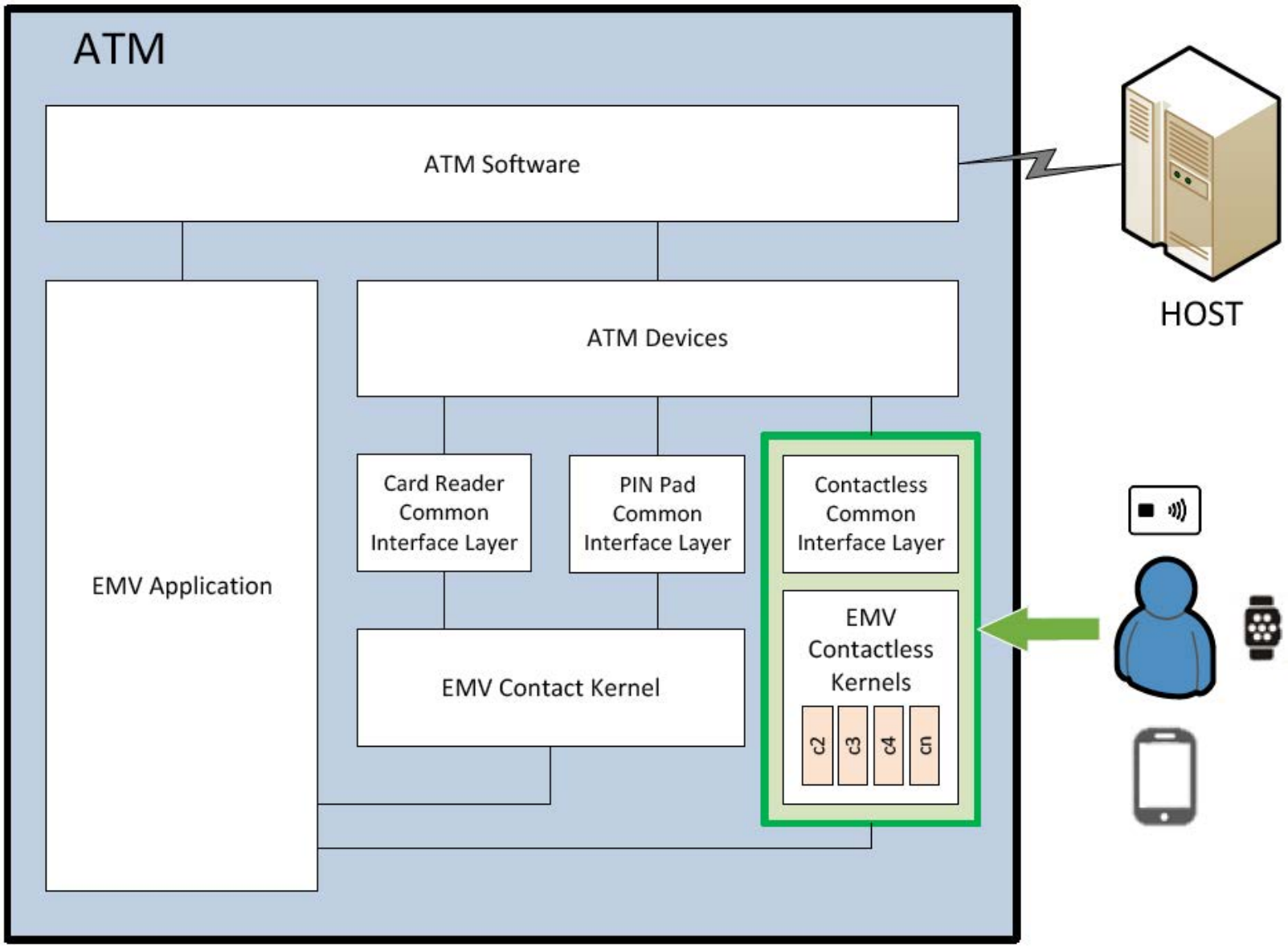
# Contactless Secure Elements Shipments worldwide (2014-2019) (in million units)




Source
Eurosmart
© Statista 2019

# Contactless Smart Payment Association (SPA) Members Shipments Worldwide (2008-2015) (in million units)

# ATM Components involved in a Contactless EMV Transaction



# Transaction Flow for ATM via a Contactless Card

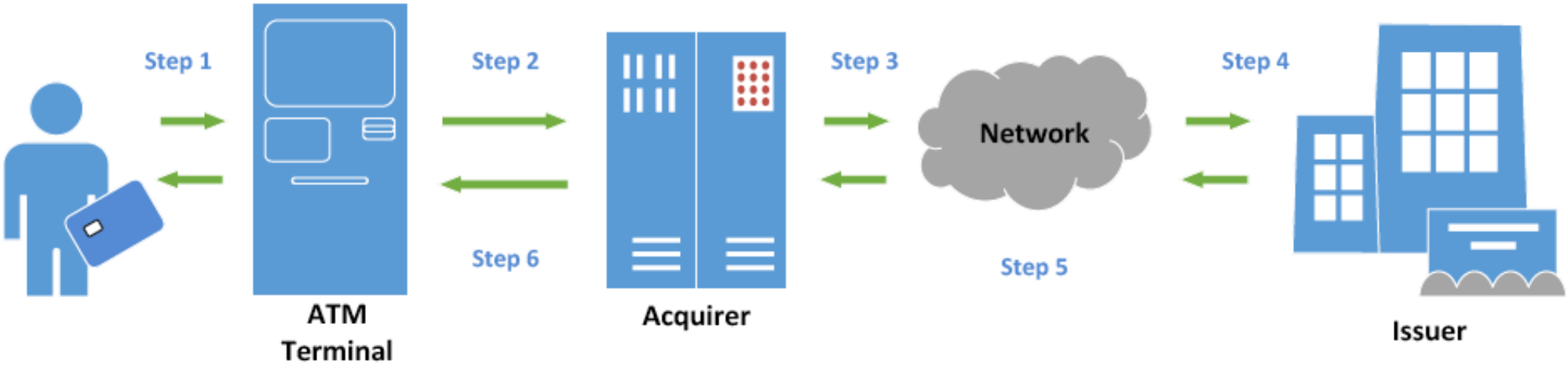
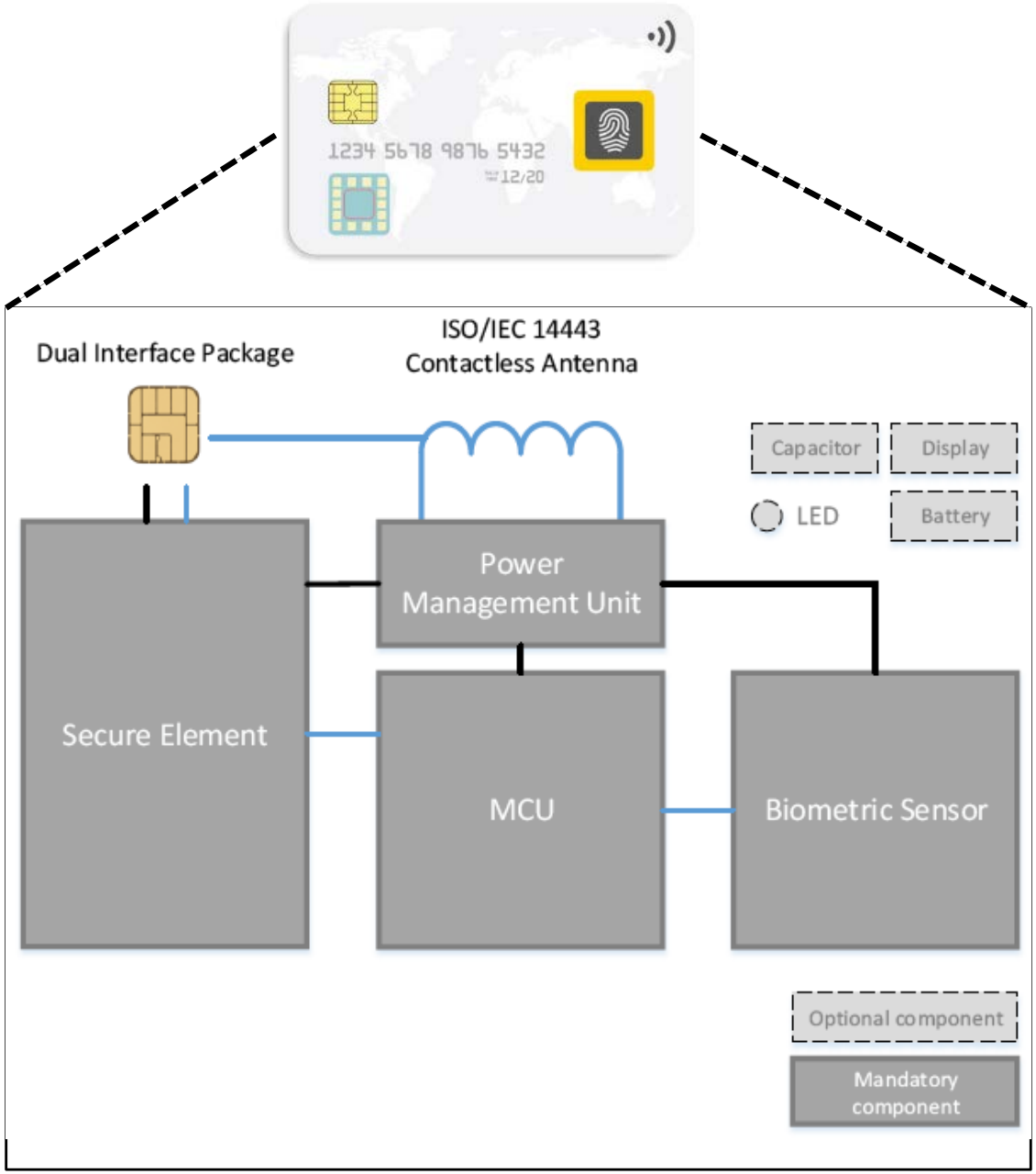


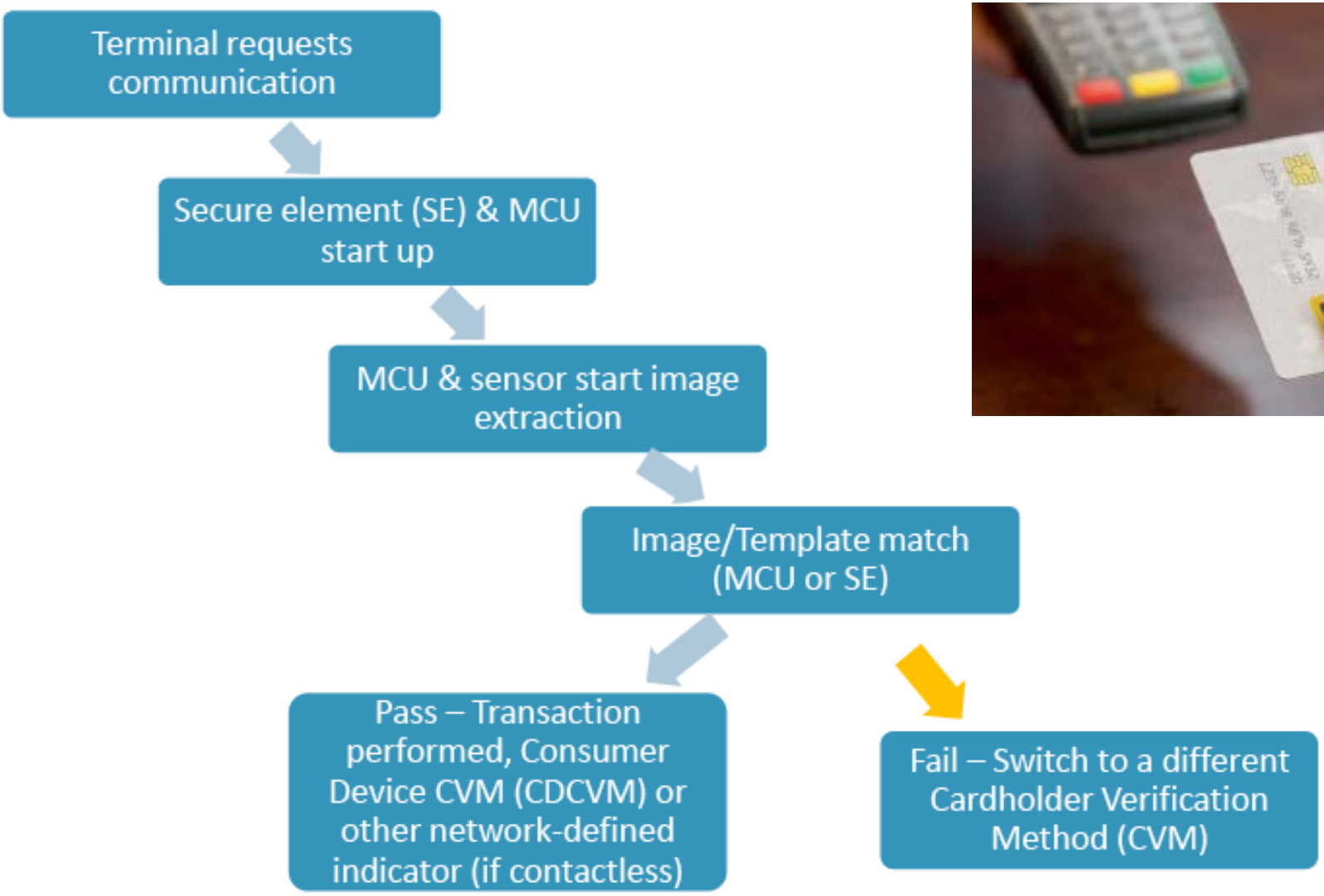

**Figure 4. Contactless Card Form Factor (i.e., Non-Tokenized) Transaction Flow**

# Emerging Trend: Biometric Card




Internal Architecture of a Biometric Card


# Operation Flow of a Biometric Cards





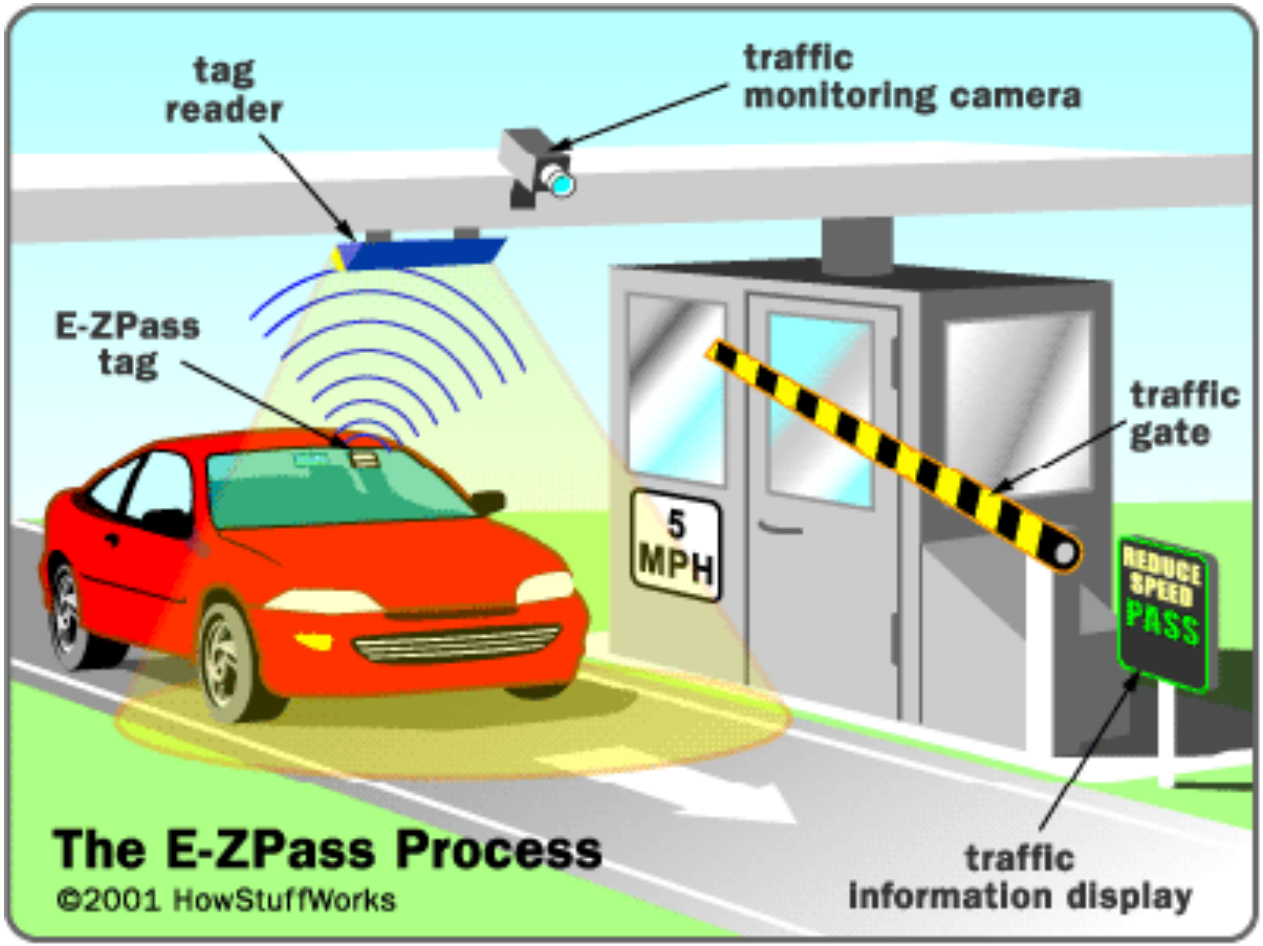

SOURCE: https://www.secureidnews.com/news-item/tech-101-contactless-smart-cards/

Speedpass

PAYMENT ON A KEYCHAIN


SMALL AND <u>CHEAP</u>

# Automated Toll Collection



# Octopus Card

- Dominant RFID payment card in HK
- Sony 13.56Mhz FeliCa RFID chip (not the ISO/IEC 14443 standards)
- Operating distance: 3-10 cm
- Bandwidth: 212 Kbit/sec
- Triple DES in 70 microsec
- EEPROM 1536 bytes
- 1KB to 64KB storage
- 128-byte data backup area
- 16-byte manufacturer ID; 16-byte issue ID
- Processing time: 50 msec on card, 300 msec overall
- Random access and cyclic files
- Anti-collision protocol

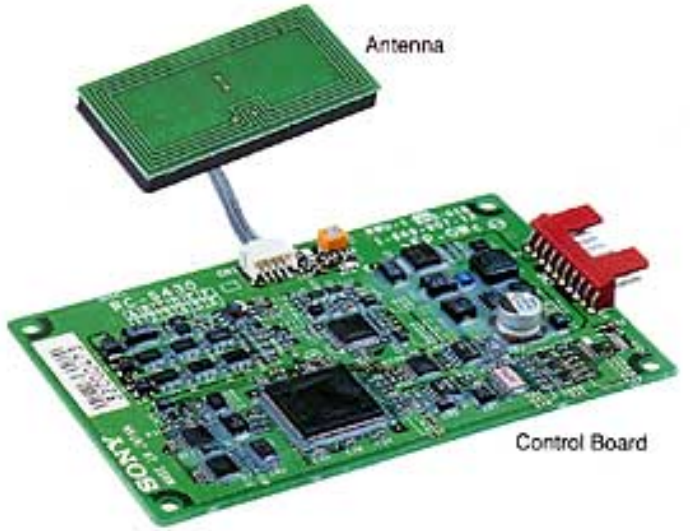

SOURCE: MITSUBISHI

# Octopus

SONY RC-S833
CONTACTLESS SMART CARD

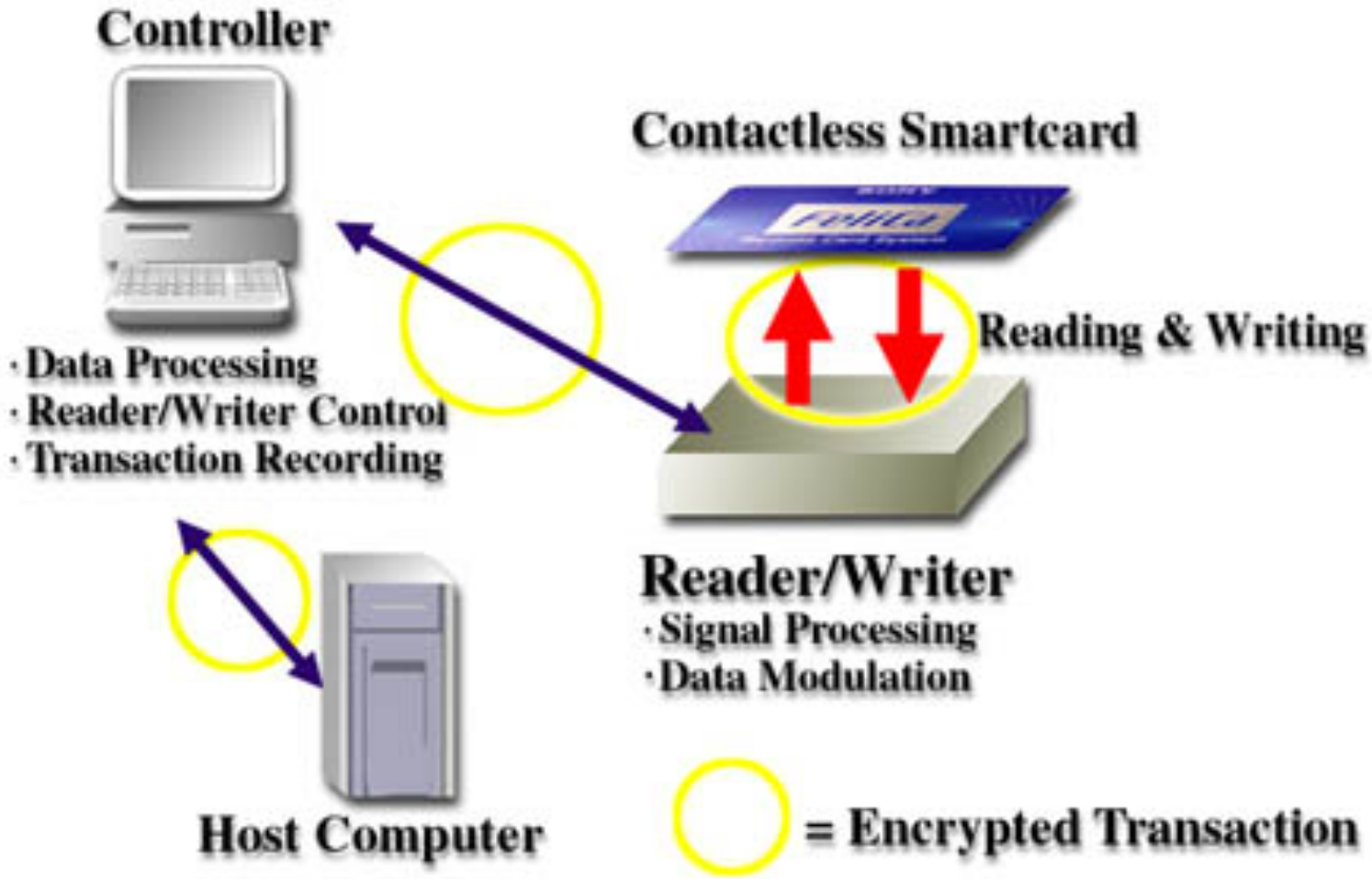

I/O SPEED: 212 Kbps

SONY READER/WRITER



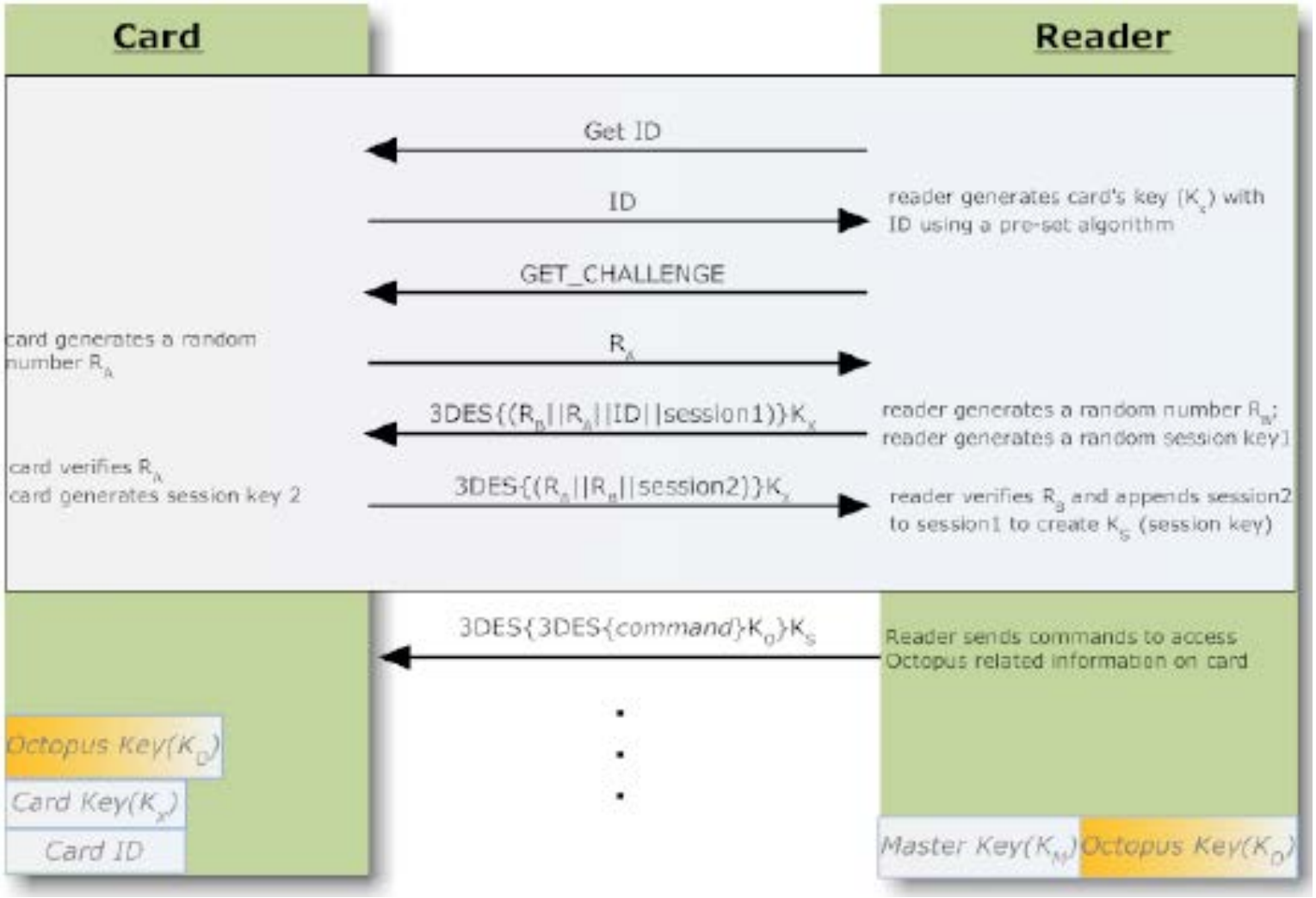

SOURCE: SONY

# Octopus Card Security



# Mutual Authentication Protocol between Octopus Card and its Reader

- 3-pass Mutual Authentication Protocol using Shared-Secret Access Key per ISO 9798-2



# Security Measures for Octopus Card

- Certified by ISO/IEC15408 EAL4
- IC Software Support
  - Card does not support software download
  - Software could not be modified once loaded

  => Reduce chance of inserting malicious logic in the software of the IC
- Data Protection
  - Cash Value
  - Backup to non-volatile memory before Write
  - Restore Immediately if the transaction is interrupted during writing
- Card Information Protection
  - Octopus Key to protect the Card's Information
  - In different stages of the card life-cycle, the key is replaced and reloaded
    - Manufacturing
    - During Shipping
    - When the cards reach the Octopus Ltd company

  => This can protect information on the card during shipping

# Business Development of Octopus Card in HK

**1997**
Contactless Chip Card Offline Payment

**1999**
AAVS

**2000**
Retail Expansion

**2003**
Go International

**2005**
Octopus Rewards

**2008**
Cobrand with Credit Card


**2011**
Cobrand with Shenzhen Tong & Lingnan Tong

**2012**
Octopus App, Transport Fare Concession


**2013**
Mobile SIM Offline Payment


**2014**
NFC Mobile Online Payment


**2015**
Octopus Service Kiosk

- Offline
- Online
- P2P
- QR Code

**2016**
O! ePay
P2P + Online Payment

**2017**
All in App + Octopus Mobile Wallet

**2018**
Global e-Commerce Partnership
+
Faster Payment Service

PayPal FPS

**2019**
Public Transport Fare Subsidy System

+
O! ePay MasterCard

八達通 Octopus | 令生活更輕鬆 Making Everyday Life Easier

# Octopus Business

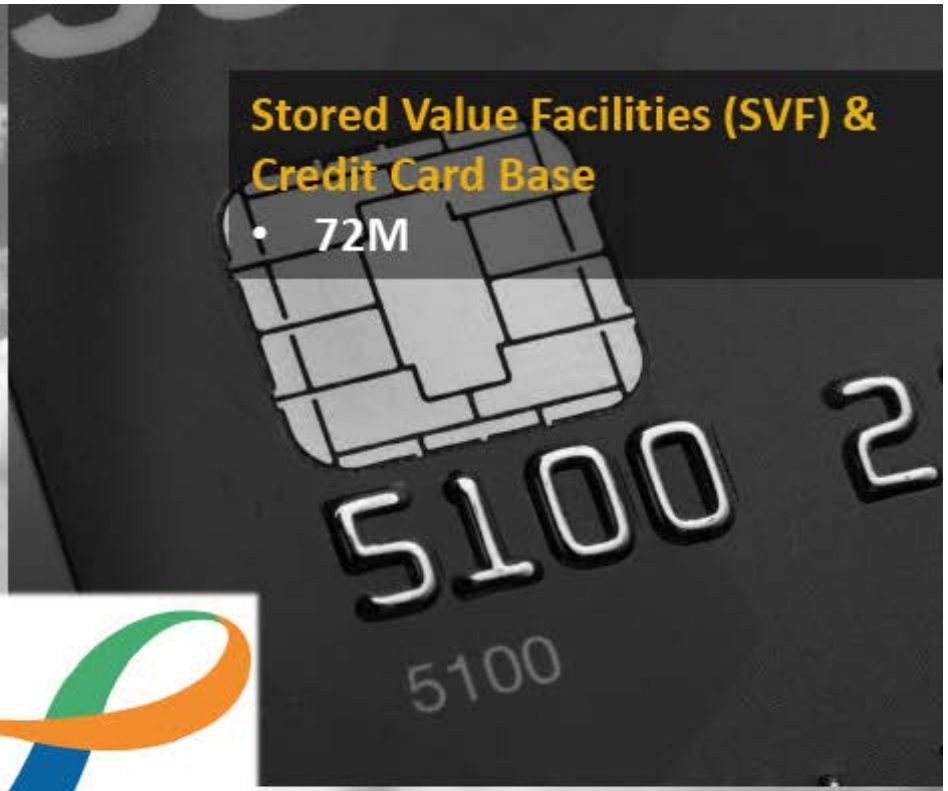
- Over 99% of HK people aged 15-64 have an Octopus card
  - 36 Million cards in circulation (circa 2020)
- 15 million transactions per day
- Daily transaction value: HK$220 million
- Accepted by 35,000 retail outlets in HK
- Transaction fees: ??HK$0.02 + 0.75%??
  - => $10 transaction costs $0.095 (0.95%)
  - Alternatively, HKT Merchant services charges 1.7% per transactions
  - (vs. 1.5% for Alipay or WeChatPay transactions)
- Applications
  - Mass Transit, Road Toll, Parking Meter, Retail Point-of-Sale, Vending Machines, Access Control, P2P payment (via OePay)
- Anonymous / personalized
- How does money get to service providers?
  - Net settlement system operated by Octopus Holdings Limited

## Estimated Market Size for Payment Business

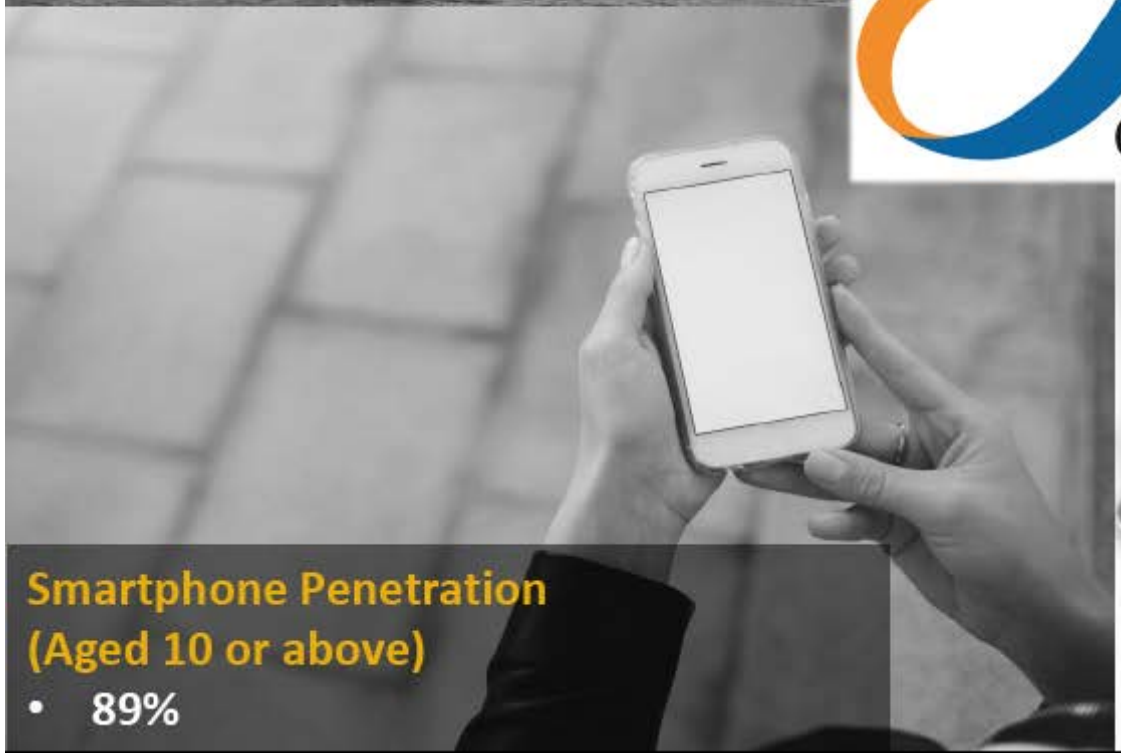
- Major Mass Transportation: HK$56B
- Retail: HK$560B

## Stored Value Facilities (SVF) & Credit Card Base

- 72M

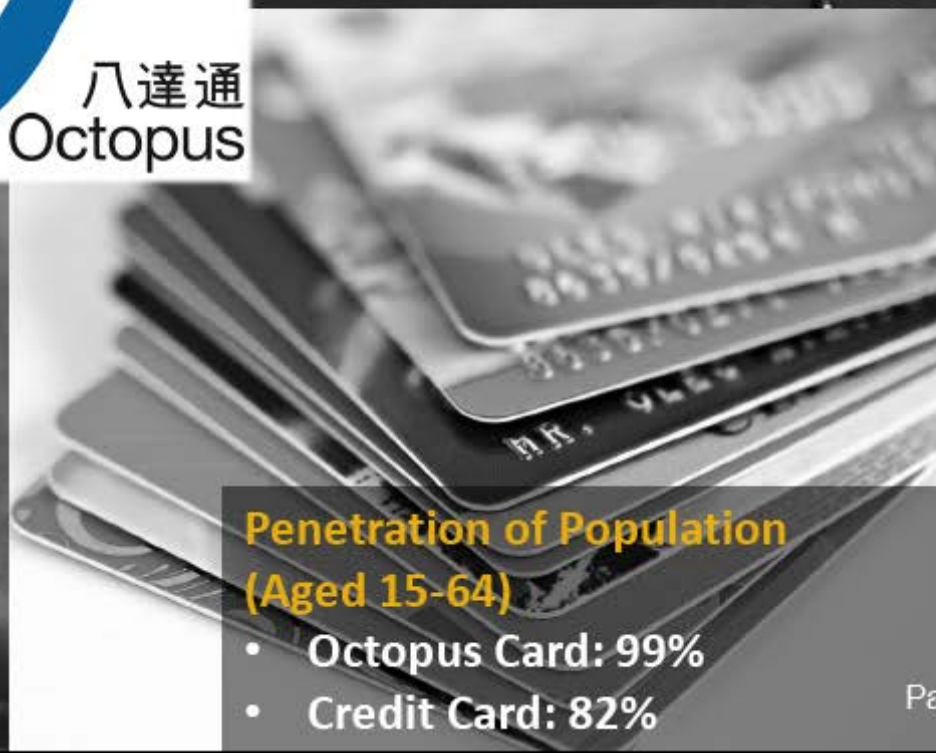



八達通
Octopus



## Smartphone Penetration (Aged 10 or above)

- 89%



## Penetration of Population (Aged 15-64)

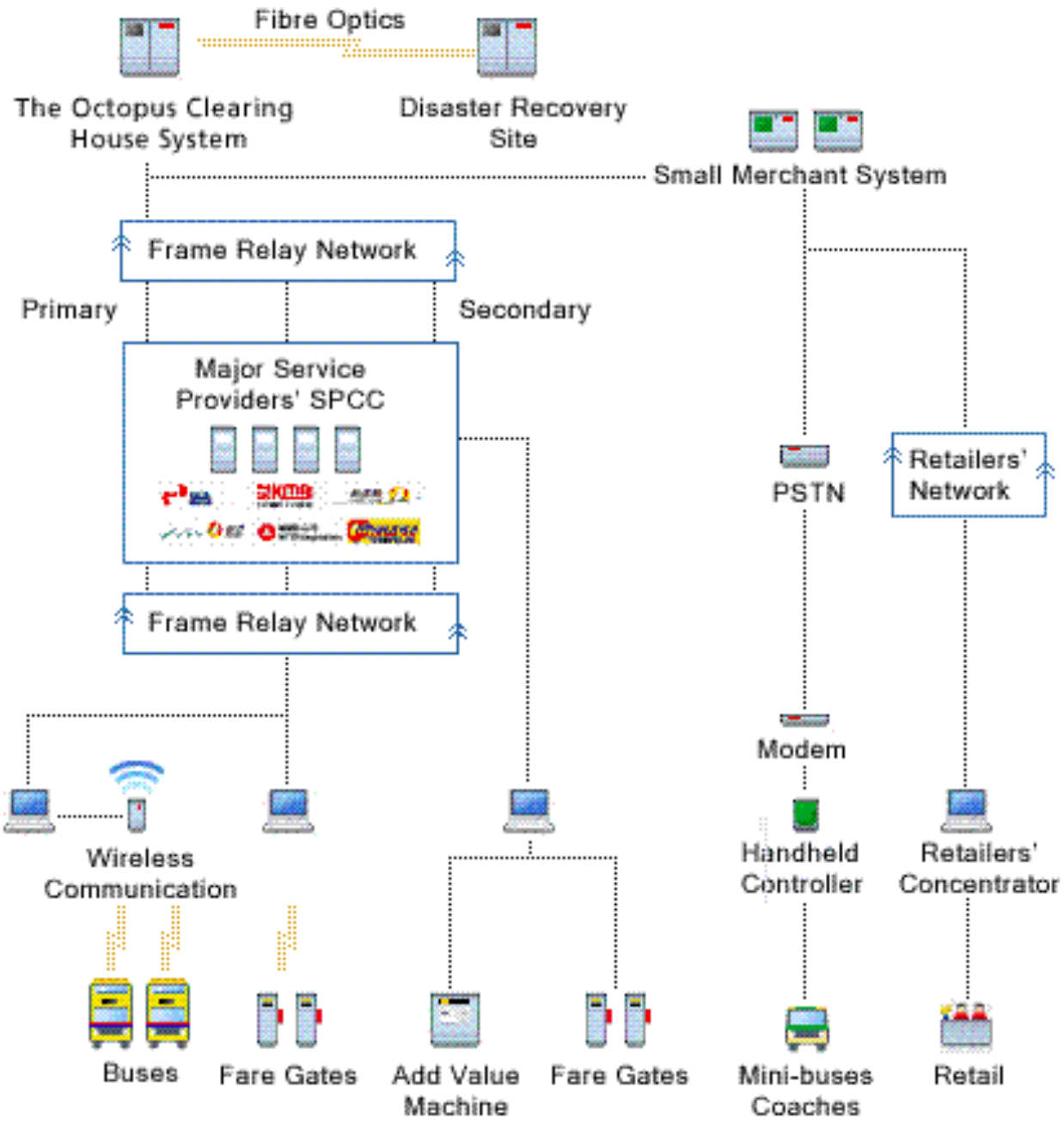
- Octopus Card: 99%
- Credit Card: 82%

# Octopus Expansion

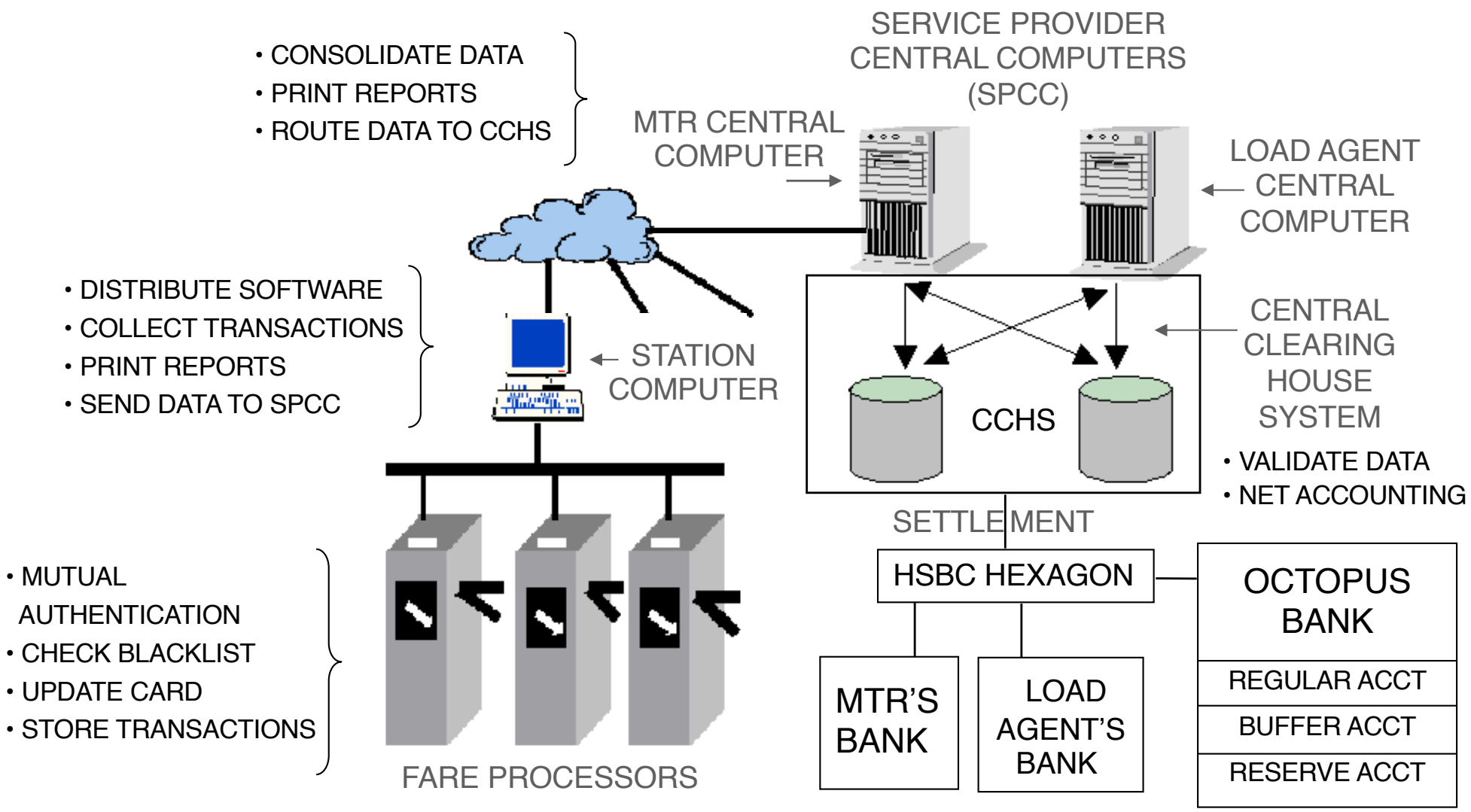
- Identity card
- Access control
- Hotel room key
- Credit card
- McDonalds
- Mobile phone
- Home readers

SOURCE: CREATIVE STAR

# Octopus System Architecture



# Octopus Settlement



# The (failed) Mondex card


- Subsidiary of MasterCard
- Smart-card-based, stored-value card (SVC)
- NatWest (National Westminister Bank, UK) et al.
- Secret chip-to-chip transfer protocol
- Value is not in strings alone; must be on Mondex card
- Loaded through ATM
  - ATM does not know transfer protocol; connects with secure device at bank
- Spending at merchants having a Mondex value transfer terminal
- Had a failed launch in HK (and elsewhere), commenced 11 months before Octopus's roll-out !

# Mondex Components (Hitachi)

Cashless ATM


PCMCIA Reader/Writer

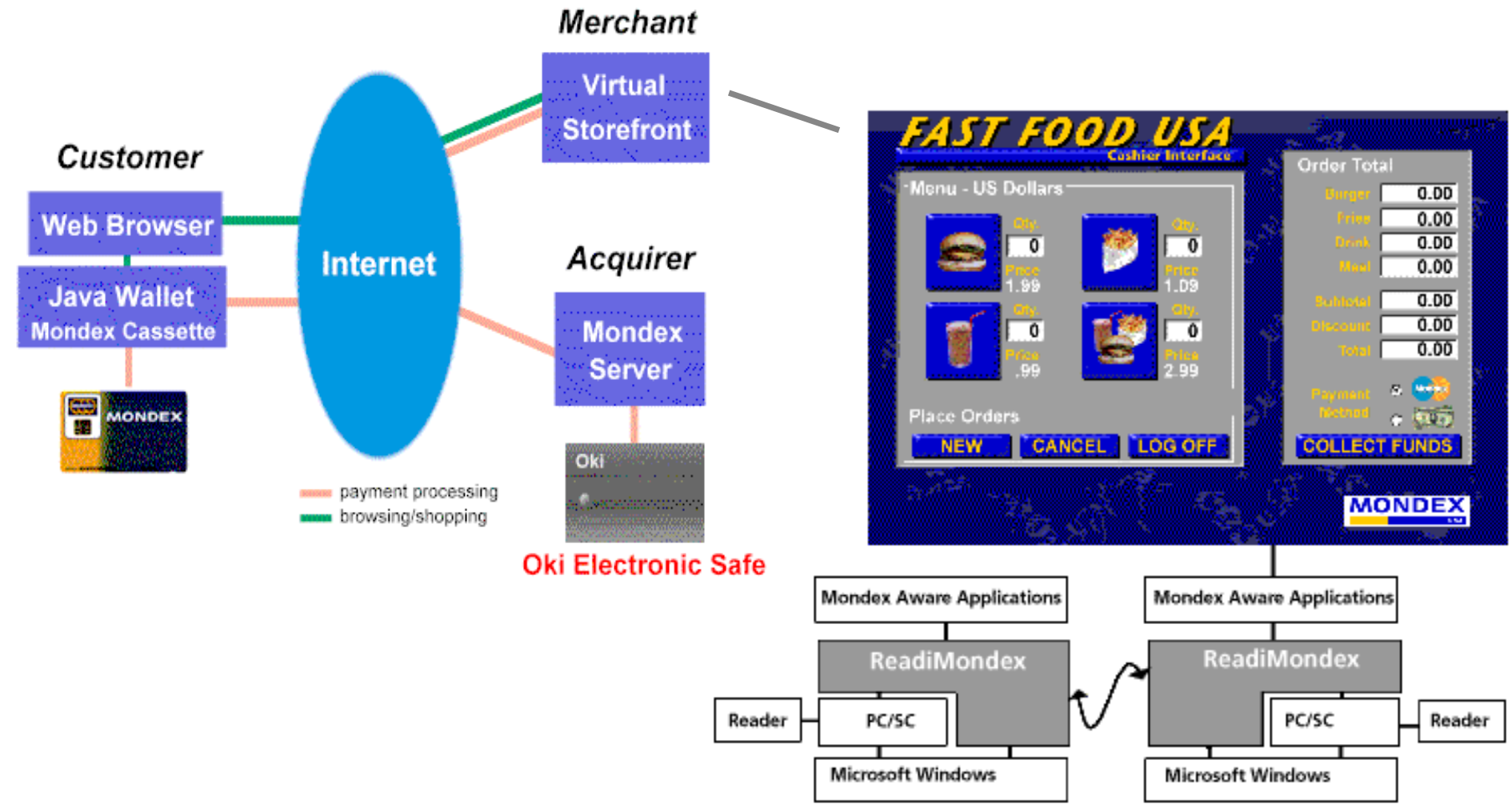

Electronic Cash Register

Electronic Wallet

Key Fob Balance Reader

SOURCE: HITACHI

# Mondex Overview




SOURCES: OKI, MONDEX USA

# Mondex Security

- Active and dormant security software
  - Security methods constantly changing
  - ITSEC E6 level (military)
- VTP (Value Transfer Protocol)
  - Globally unique card numbers
  - Globally unique transaction numbers
  - Challenge-response user identification
  - Digital signatures
- MULTOS operating system
  - firewalls on the chip

# Two different Fates: Octopus vs. Mondex in HK

**Table 1: Background of the two electronic payment systems**

| | Mondex | Octopus |
|---|---|---|
| Founding members | Financial sector<br>HSBC, Hang Seng Bank, Mastercard International | Transport sector<br>Creative Star – joint venture between five transport companies |
| Local market share | HSBC issues 64.4% of Hong Kong's currency (2002) [14]<br>HSBC and Hang Seng deposit 32.5% of Hong Kong's M2 money supply (2001)[3] | Mass Transit Railway (MTR): 11 million passenger journeys per day (total population was 6 million) |
| System cost | Information unavailable | US$53 million |
| Issuer | Licensed banks | Authorized deposit-taking organization (2000) |

Source:
Leung Sea, Lucia SIU, "Coercing consensus: unintended success Of the Octopus electronic payment system," PISTA IMSCI 2008.

# Two different Fates: Octopus vs. Mondex in HK

**Table 2: Outcome of user acceptance**

| | Mondex | Octopus |
|---|---|---|
| Cards issued | Pilot phase, trial quantity (1996)<br>0.19 million (Nov 1998) [6] | Pilot phase, trial quantity (1997)<br>4.6 million (Nov 1998) |
| | Below 0.1 million (Feb 2002) [13] | 9 million (Feb 2002) [21]<br>17 million (Jun 2008) |
| No. of merchants | 8000 [6]<br>Most are retail shops | 120 (2002) [21]<br>Most were conglomerate chains<br>Over 2000 (Jun 2008) |
| Daily transactions | Not disclosed | Over 7 million (Feb 2002) [21]<br>Over 10 million, turnover HK$85 million (Jun 2008) |
| Profit | Never attained profit | HK$18 million (2000) [20] |
| Outcome | User resistance<br>Low usage<br>HSBC sold out all shares<br>Hong Kong project terminated (2002) [1] | City-wide acceptance<br>High regular turnover<br>HKMA released previous 15% restriction on non-transport purposes (2000) [21] |

Source:
Leung Sea, Lucia SIU, “Coercing consensus: unintended success Of the Octopus electronic payment system,” PISTA IMSCI 2008.

# Two different Fates: Octopus vs. Mondex in HK

**Table 3: Comparison on technical and marketing merits**

| | Mondex | Octopus |
|---|---|---|
| User cost | (+) Free (HK$100 fee waivered) | (-) HK$50 deposit (US$6.41) |
| Legal Status | (+) Full legal status of money | (-) Limited legal status / area of use |
| Launching time | (+) Oct 1996 | (-) Sep 1997 |
| Privacy concern | (-) Holds personal information, linked to bank account | (+) Contains no personal info<br>(Later on optional varieties linked up with bank accounts and award programs) |
| Contact mode | (-) Need contact to read/write | (+) Contactless read/write |
| Speed | (-) Read/write time: 5 seconds<br>Date transmission: 9.6 kbit/s | (+) Read/write time: 0.3 seconds<br>Data transmission: 212 kbit/s |
| Specifications | MULTOS chip<br>Patented issuance and update mechanism: STEP (Secure Trusted Environment Provisioning)<br>Verification and encryption: KMA (key management authority) | Sony 13.56 MHz RFID (FeliCa radio frequency identification) chip<br>Proprietary standard predating the ISO/IEC 14443 standard<br>ERG (Australian) as system integrator<br>PKI (public key infrastructure) encryption<br>Two-way authentication |

(+) Merit (-) Disadvantage

Source:
Leung Sea, Lucia SIU, “Coercing consensus: unintended success Of the Octopus electronic payment system,” PISTA IMSCI 2008.

# Major Ideas

- Embedded-microprocessor-based Smart cards prevent skimming attacks as the user secret/ key never leaves the card and difficult to be reversed engineered
- Powerful microprocessors allow
  - Cryptography ; certificates, authentication ; secure SVFs/wallets
- EMV standards as well as Liability-Shift policies speed up adoption of EMV-chip payment cards worldwide.
- Wireless (Contactless) cards enable new business models and competitive advantages
  - Require updates of Merchant-side devices as well
  - Contactless card is just one of the many solutions for Mobile Commerce;  Alternative technologies/ Solutions keep coming, e.g. NFC, Tokenization, QR code, etc ;
  - Different Technologies has different implications on who have more control on the ecosystem: e.g. Card Issuers, Mobile Service Providers, BigTech companies, etc