CONTACTLESS SMART CARDS FOR TRANSIT
AGENDA

- Discussion of plastic cards
- Contactless smart cards now
- Contactless smart cards in the future
- Future technologies
CARDS AND TICKETS

• Construction
  • PVC – Polyvinyl Chloride - Standard card material
  • Composite PVC+PET (Polyester) – recommended for reverse-transfer printing and overlamination
  • Polycarbonate – Driver licenses, laser printing
    • Durable, but more expensive than PVC
  • Biodegradable plastics
    • Only effective in certain configurations
  • Paper tickets
• All can have mag stripes
CARD CONSTRUCTION
Chip Inlay Layer
CARD CONSTRUCTION

Mag Stripe Layer
CARD CONSTRUCTION

Pre-printed Layer
LAYERS OF A SMART CARD

AzTA 2013_Contactless Smart Cards
CARD LAMINATING PRESS
IDENTIFICATION TECHNOLOGIES

• THE CARD HOLDS IDENTIFYING NUMBERS FOR ALL THE APPLICATIONS THAT IT TOUCHES

• EXTERNAL
  • Visual
    • Printed Image
    • Photo
    • Printed Number
  • Automatic ID
    • Encoded Mag Stripe
    • Bar Code

• INTERNAL
  • Automatic
    • Prox Chip
    • Contactless Chip
    • Contact Chip
VISUAL SECURITY

A. Extremely fine line Guillocche elements
B. Animated Light Micro-Text
C. Flip Image - Two Channel Hologram
D. Laser Retrievable Image
E. Red UV Print
F. Fine Lines
G. Micro-Text
H. Red UV Print
I. Fine Lines
J. Micro-Text
HOLOGRAPHIC OVERLAMINATE

Custom Micro Text
This microscopic type is so detailed, it cannot be duplicated via dye-sublimation, ink jet or laser printers. Here, Globe Labs has strategically placed “GLOBE LABS CLASSIFIED” in a designated area within the Fine Line Design (Guilloche). This is an excellent covert feature for authenticating an ID.

Custom Pseudo Color
An effective and attractive element that is difficult to duplicate, yet very easy to verify. Tilt the card one way, and you see metallic, holographic tones in your image. Tilt it again and you see saturated, true colors along with atomic numbers and other details. In this example image, the card is angled to show the many varying bright colors of the noble gases from the periodic table.
BAR CODES

- Linear Bar Code
- 2-D Bar Code, PDF-417 (Driver licenses, Real ID)
- QR Bar Code - payments
MAGNETIC STRIPES

• 1, 2 or 3 tracks for main stripe
• HiCo (2750-4000oe) is common
• LoCo (300-600oe) is mostly for hotel keys
• Inexpensive and easy to encode
• Easy to replicate
DEFINITIONS - RFID

Three frequency ranges used for Radio Frequency Identification cards:

1. Low Frequency – “Prox”
2. Ultra High Frequency – “UHF” “RFID” “EPC Gen II” (Electronic Product Code)
3. High Frequency – “Contactless” Smart Card
**PROXIMITY CARDS**

- **Proximity**
  - “Prox” “Proxy cards”
  - 125KHz, “Low Frequency”
- **25 year-old technology**
- **Vulnerabilities**
  - New mobile devices that can read and write to Prox cards
  - Soon it will be easier to clone Prox than mag stripes
- Not normally used for transit applications
“RFID”

- Used as ID tags for things more often than people
- EPC Gen2– Electronic Product Code
- 30’ Read range
- 880-930 MHz, “Ultra High Frequency (UHF)”
- Inventory tracking
- Vehicle payments – tolls, parking
- Passports
CONTACTLESS CARDS

- 13.56 MHz “High Frequency”
- Additional rewritable memory available, up to 8K bytes
- Advanced security available - encryption
- Widely used for physical access, transit, payments
TRANSIT CARDS – PAST AND PRESENT

• Fujitsu
  • Chicago Transit Authority (CTA)
  • Washington Metro Area Transit Authority (WMATA)
• MIFARE
  • Philips – now NXP
  • Internationally used since early 1994
  • Usually used in offline mode for transit (read/write at turnstile)
  • Security of MIFARE Classic now known to be compromised
TRANSIT CARDS – PRESENT AND FUTURE

- NXP chips
  - MIFARE Ultralight
  - MIFARE Classic
  - MIFARE Plus
  - MIFARE DESFire EV1
- HID
  - SEOS
    - ISO 14443 microprocessor
- Open loop
  - Visa PayWave
  - MasterCard PayPass
CHIPS AND ...

- Plastic cards
  - Can be made with any chip
- Paper tickets
  - Can be made with many chips
  - Often MIFARE Ultralight
- Any card or paper ticket can have mag stripe
CONTACTLESS MEMORY

For commercial contactless cards:
Memory on a contactless chip is like a hardcover book
• Book cover has the Card Serial Number (CSN) or Universal ID (UID)
  • Unique to every contactless chip
  • Electronically “stamped” by the mfr.
  • Interoperable
  • No data encryption
For commercial contactless cards:

- The first chapter of the book can be reserved for the physical access application
  - Card ID number, for physical access readers
  - Locked with manufacturer’s key
  - Recommend unique encryption key for each institution
  - Normally non-rewritable area
CONTACTLESS MEMORY

For commercial contactless cards:
• Remaining chapters can be used for other applications
• “Putting an application on the card”
  • Storing a number in an area of the chip memory for retrieval by a particular application
  • Each application has its own chapter
  • Often rewritable
  • Biometric templates, payment data
CONTACTLESS NUMBERS REVIEW

- CSN, UID, CHUID – Free read, not very secure
  - Used by unlicensed reader manufacturers
- Physical access control application number
  - Encrypted, secure
- Other application numbers
  - Contactless credit card payment data mimics mag stripe data
  - Transit applications usually proprietary to system
- Read/write data
  - Some physical access control applications
  - Transit fare collection systems
  - Payment applications – increment, decrement
THE FUTURE -- PHONES!

• NFC for physical access
  • Near Field Communication
  • Contactless chip in the phone that talks to phone OS
• Not many phones with NFC chips yet
• Depends on payment applications
• After market NFC add-ons
  • SD card
  • SIM
  • Case with NFC chip and antenna
• Many business hurdles to overcome
NFC FOR REAL

• Japan and Korea
  • FeliCa
    • NTT DoCoMo
    • Sony
• London
  • Just getting underway
• Salt Lake City and Austin
  • Pilots
• Many other small pilots
NEW TRANSIT IMPLEMENTATIONS

- Account based, not stored value on card
- UTA
  - Reading CSN from many cards
  - Allows local businesses, ski hills and universities to use their existing cards (iCLASS, MIFARE, DESFire, mag stripe)
  - “Honor system”
- CTA
  - Open loop system - MasterCard Pre-paid
  - White label cards available for institutions
  - Cannot use customers’ existing contactless cards (at least not yet)
- MBTA
  - Programming MIFARE chips in MIT’s cards
PERSONALIZING CARDS
PRINTING ON CONTACTLESS CARDS
PRINTING ON CONTACTLESS CARDS

Reverse Transfer Card Print
REVERSE TRANSFER PRINTERS
CREDENTIAL CONCLUSIONS

• Determine your requirements and policies
  • Levels of security
  • Throughput
  • Convenience
  • Human participation
• Readers are almost forever – choose wisely
• Create migration path to introduce advanced contactless technology
  • Multi-technology cards and/or readers
• Visual security for cards is important
• Keep systems that work well and make sense
• Test!
Questions?

Call or email me for more information.

David Stallsmith
Director of Product Management
704-897-1156
david.stallsmith@colorid.com