

C O L O R I D

# COLORID CAMPUS IDENTITY SUMMIT

## CURRENT TECHNOLOGIES

**Danny Smith**

Executive Vice President, ColorID

**Todd Brooks**

Director - Product Management, ColorID

**Tim Nyblom**

Director – Education Group, ColorID

**Brian English**

Account Manager – Education Group, ColorID

**Mark Degan**

Director – Corporate Marketing, ColorID



C O L O R I D

# AGENDA

Card Technology

Legacy Cards

Contactless Cards

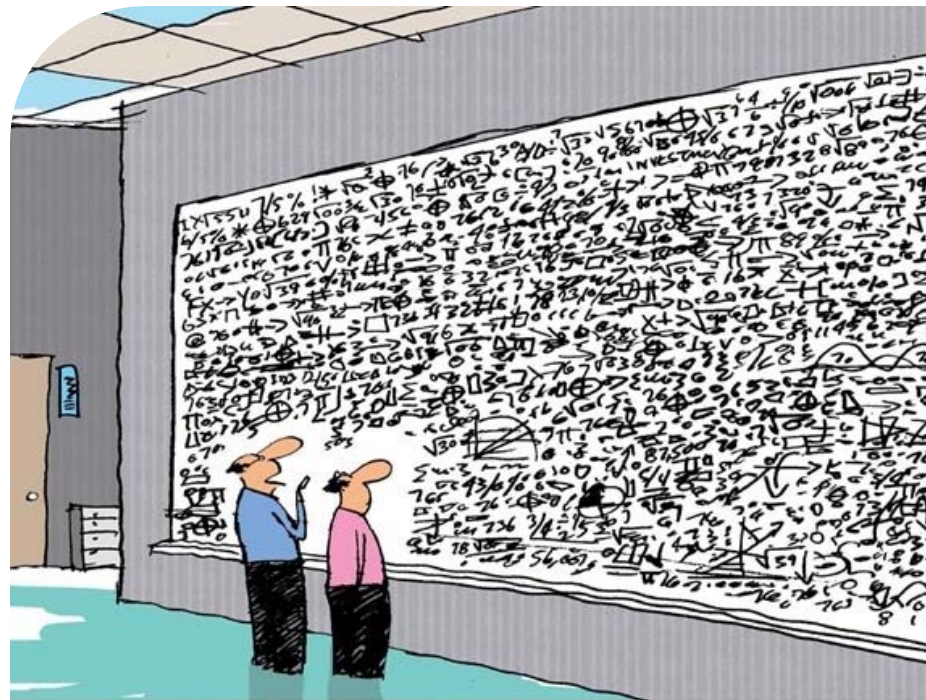
Contact Chip Cards

Physical Access

# AN INTRODUCTION TO CARD TECHNOLOGY

Fundamentals of Card Technology

# COLORID



"...and that, in a nutshell, is how we get to a current, secure student ID..."

# COLORID DEFINITIONS

Frequency	The cycles/second of a radio frequency. How quickly the wave oscillates over a period of time. Like radio stations (88.1- 108 MHz)
Keys	Much like a key to a house, a digital value that “unlocks” data i.e. the key or password to decrypt
Data	In terms of access control cards, binary or hexadecimal values representing a card holder’s identification number. Common structure is 26 bit, Corp. 1000, 37 bit, etc.
Encryption	Data security. The act of creating a value that is unintelligible to an unauthorized viewer
PACS	Physical Access Control System
Prox	Low Frequency, 125 KHz RFID Card
Contactless or Smart Card	High Frequency, 13.56 MHz RFID Card
Wiegand	Lots of Meanings > Card Format > Type of Card > Wiring Protocol

C O L O R I D  
IDENTITY

WHO ARE  
YOU?

# COLORID STAGES OF IDENTITY



ESTABLISH  
IDENTITY



CREATE SYSTEM  
IDENTIFIER –  
“CREDENTIAL”

- Something you know
- Something you have
- Something you are



TRUST THE  
SYSTEM

- Input device for credential
- Database
- System decision per application

# WHY IS IDENTITY IMPORTANT?

## Access rights

- Physical
- Logical

## Services and benefits

- Classes
- Food and housing

## Financial transactions

- POS



# IDENTITY – WHAT CAN GO WRONG?

## Risks of incorrect identity

- Accidental
  - Incorrect billing, grades, etc
- Impersonation
  - Criminal behavior
    - Physical harm
    - Property theft
    - Property damage
  - Compromise of information systems



Once established, identities persist

# COLORID AUTOMATED IDENTIFICATION



Auto-  
identification  
methods

PINs,  
Passwords

Cards

Tokens

Phone-based  
systems

Biometric  
capture  
systems

# LEGACY CARD TECHNOLOGIES

Magnetic Stripes, Barcodes, Prox

# COLORID IDENTIFICATION: SURFACE TECHNOLOGIES



## Visual

Printed  
Image

Photo

Printed  
Number

Security Features  
(Holograms, Foils, UV  
Images)

## Bar codes

Can be  
printed on  
any card

1-D  
2D  
QR

Standard for  
libraries

Variety of  
bar code  
fonts

Security:  
Easily  
copied

# COLORID IDENTIFICATION: SURFACE TECHNOLOGIES



Mag  
stripes

Available on any  
type of card

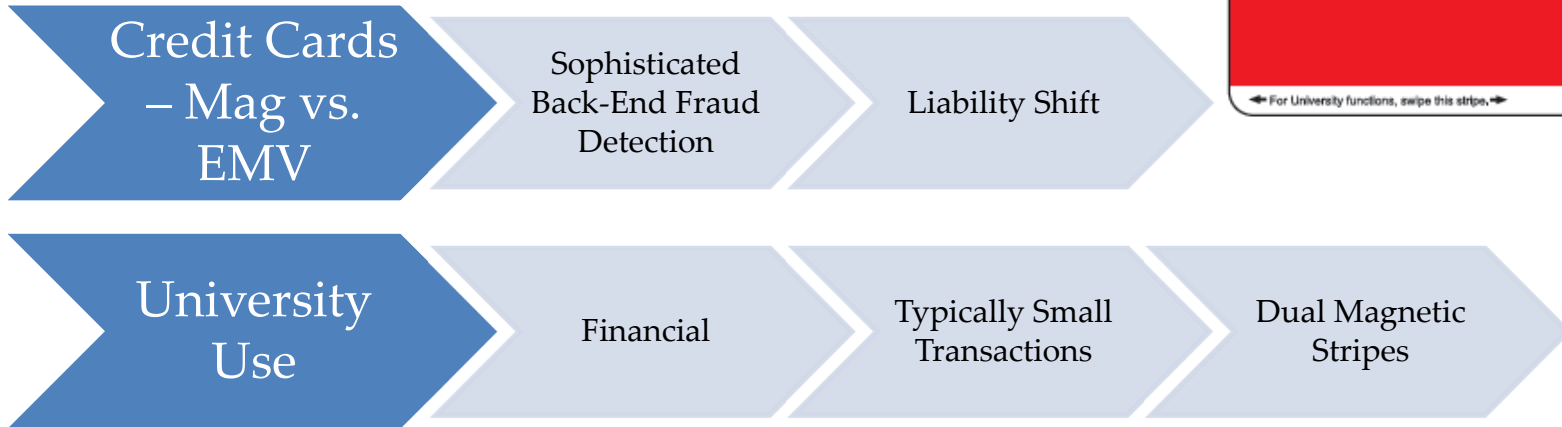
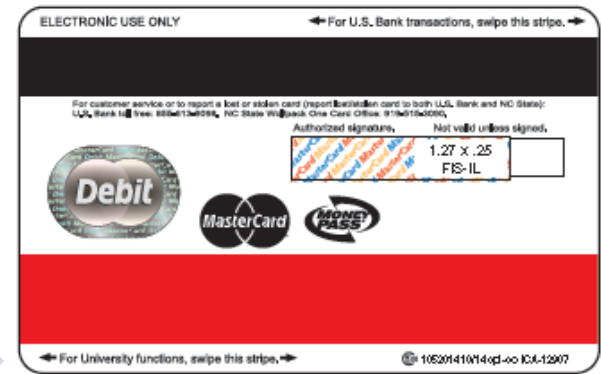
1, 2 or 3 tracks

1 or 2 mag  
stripes

Mag stripes are  
normally  
encoded in ID  
printer

Security: Easily  
cloned

# COLORID MAGNETIC STRIPE

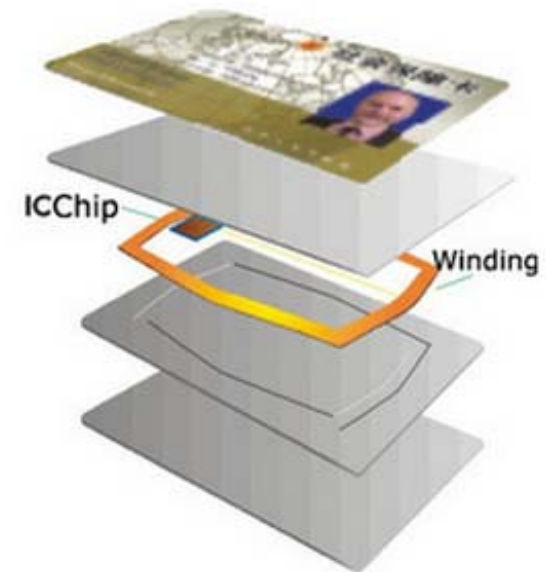
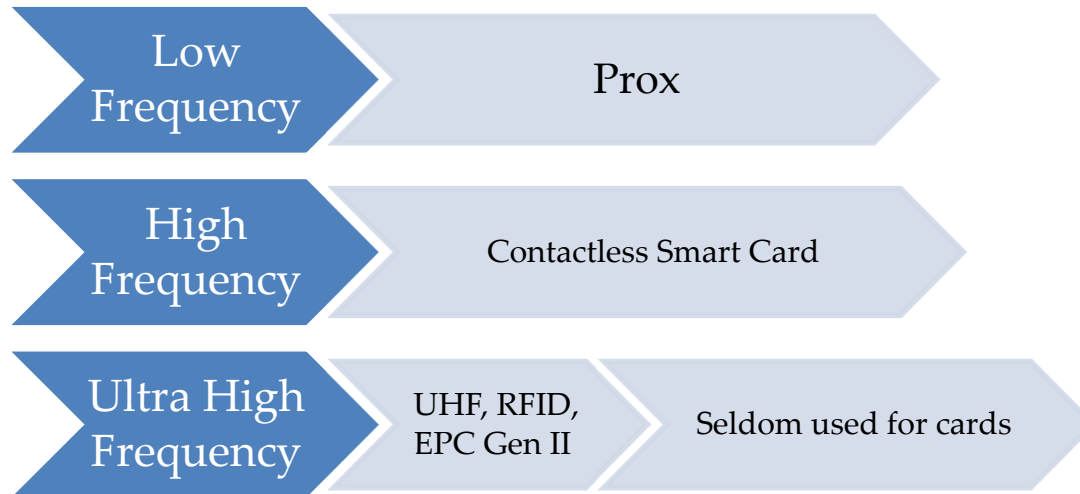


# COLORID RFID CARDS



R.adio F.requency I.D.entification

Three primary frequency ranges:



# COLORID PROXIMITY

## Prox

- 125KHz, Low Frequency
- Up to 100 bits of memory
- Vulnerability
  - 25 year-old technology
  - No Encryption - Cloning



# COLORID PROX CONTEMPORARIES



- So, why should I consider migrating from Prox. Well.....

## Cloning A 125 kHz Proximity Card

# COLORID PROX CLONING

## Bump and clone: Do ID badges put college campuses at risk?

-Georgia Institute of Technology  
-Northern Arizona University



\$35 on Amazon



[www.clonemykey.com](http://www.clonemykey.com)

© 2018 -- IDENTITY ROADMAP -- ColorID, LLC



Long-Range In A Briefcase

# CONTACTLESS CARDS

1<sup>st</sup> Generation: Mifare Classic, Legacy iClass

# COLORID CONTACTLESS SMART CARDS

13.56 MHz “High Frequency”

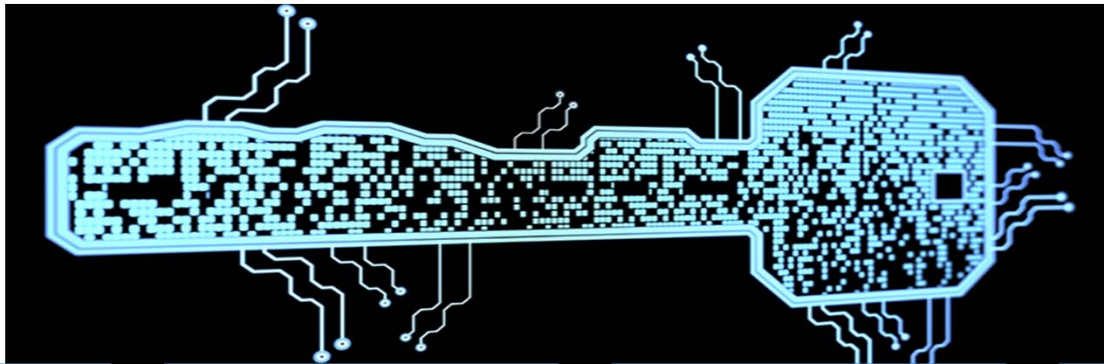
Advanced security available – data encryption

Additional memory, up to 32K bytes

Widely used for physical access (Driver), transit, payments



# COLORID CARD DATA SECURITY



## Card data security relies on encryption

- Turns data into unrecognizable form
- Common Algorithms:
  - Crypto1
  - DES
  - 3DES
  - AES

## Encryption keys or keysets

- Card data encrypted with the key
- Reader knows the key and can decrypt data
- Mutual authentication between card & reader
- Custom keys available

## Secure readers and cards typically from same manufacturer

- Reader holds the keys for the cards it reads
- HID → HID
- Allegion → Allegion
- Bb → Bb

## Most contactless card data is static

- Must be encrypted at rest and in transit
- Original transit apps used value stored on card

# CONTACTLESS CARD DATA

## Contactless Protocols

- ISO 14443
- ISO 15693
- Card Serial Number (CSN/UID)
- Not Encrypted

## Secure Data

- Typically PACS data 26-78 bits
- Parsed into Facility Code, ID, other
- Managed Formats (Corp 1000, U1000, CardTrax)

## Additional applications

- Any type of data required
- Many use cases

# COLORID CONTACTLESS CARD PROVIDERS

## HID

HID prox  
introduced in  
1980s

iCLASS - 2003

“SIO” for iCLASS,  
MIFARE, MIFARE  
DESFire EV1 –  
2012

SEOS - 2014

## Allegion

Originally XceedID, Ingersoll Rand, then spun off - 2013

- XceedID Prox
- aptiQ: MIFARE, MIFARE DESFire EV1

## Generic

MIFARE, DESFire EV1 (custom keys / applications)

# COLORID MIFARE CLASSIC

## MIFARE CLASSIC

- Developed Mid-1990s by NXP (formerly Philips Electronics)
- Originally Intended for Transit
- Proprietary Algorithm for Encryption – Crypto1
- Algorithm Hacked
- New – Mifare Classic EV1



# COLORID HID ICLASS

## HID iClass

- Released in 2003
- Primarily for Physical Access
- ISO 15693 – Longer Read Range
- Pico-Pass Chipset
- DES or 3DES Encryption
- iClass Hack – Keys available on internet
- Elite key also vulnerable



# C O L O R I D

\$250 - \$350

Readily Available, No Skill Required

Low Frequency and High Frequency

Hack Mifare Classic Keys

Duplicate Prox Cards

Emulate Cards, CSN

Chinese MAGIC Cards



# CONTACTLESS CARDS

2<sup>nd</sup> Generation: Mifare DESFire EV1, iClass SE

# COLORID

## SIO ENABLED (SE)

### HID SIO Secure Identity Object

- SIO Data can be anything
- Can be preprogrammed by HID
- Loaded with AsureID software or Over the Air (OTA) to mobile
- AES encryption, digital signature, bound to device
- SIO read at door by HID SE readers
- iClass SE, DESFire SE, Mifare SE



# COLORID DESFIRE EV1

## Secure Multi-application Platform

- AES-128 Encryption
- PICC Master Key – Card Level
- Flexible application and file system
- Each application like a folder in Windows
- Applications and files defined during creation
- Each application manages its own keys
- Access rights defined per file



# CONTACTLESS CARD APPLICATIONS

What can my card do?

# COLORID CARD APPLICATIONS

- Contactless  
Cards can store many applications
- Similar in concept to apps on a smartphone



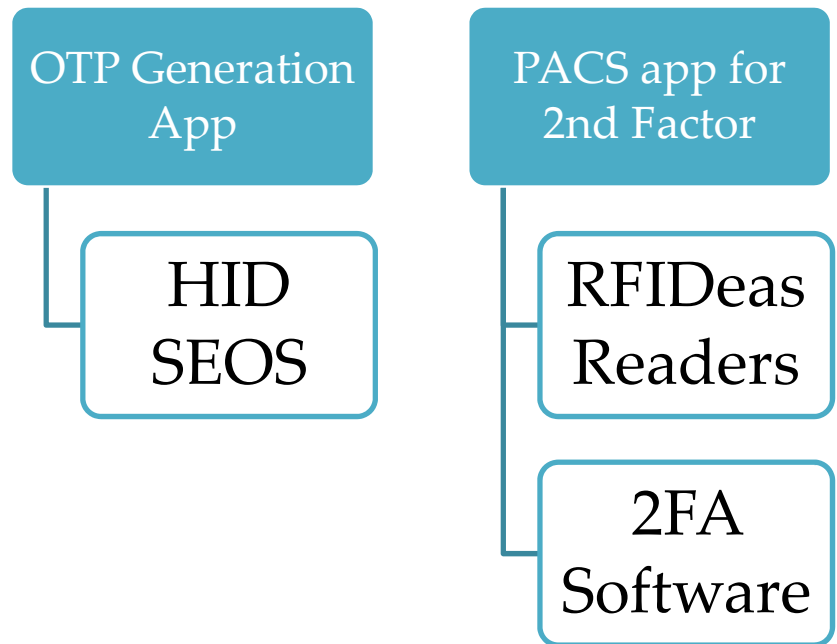
# COLORID APPLICATIONS - TRANSIT



## Transit

- Separate application – typically for NXP cards
- Sometimes read UID only

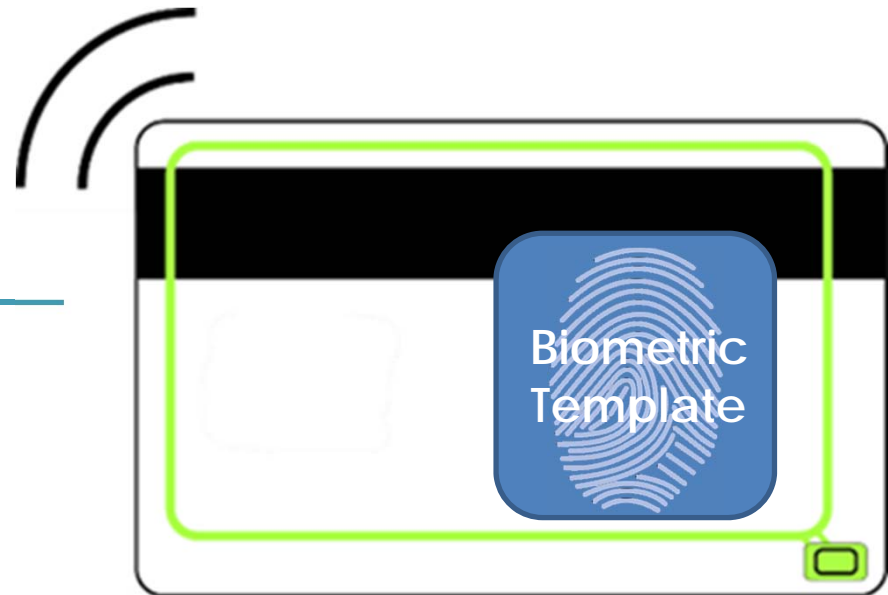
# APPLICATIONS - LOGICAL ACCESS



## APPLICATIONS – STORE BIOMETRICS

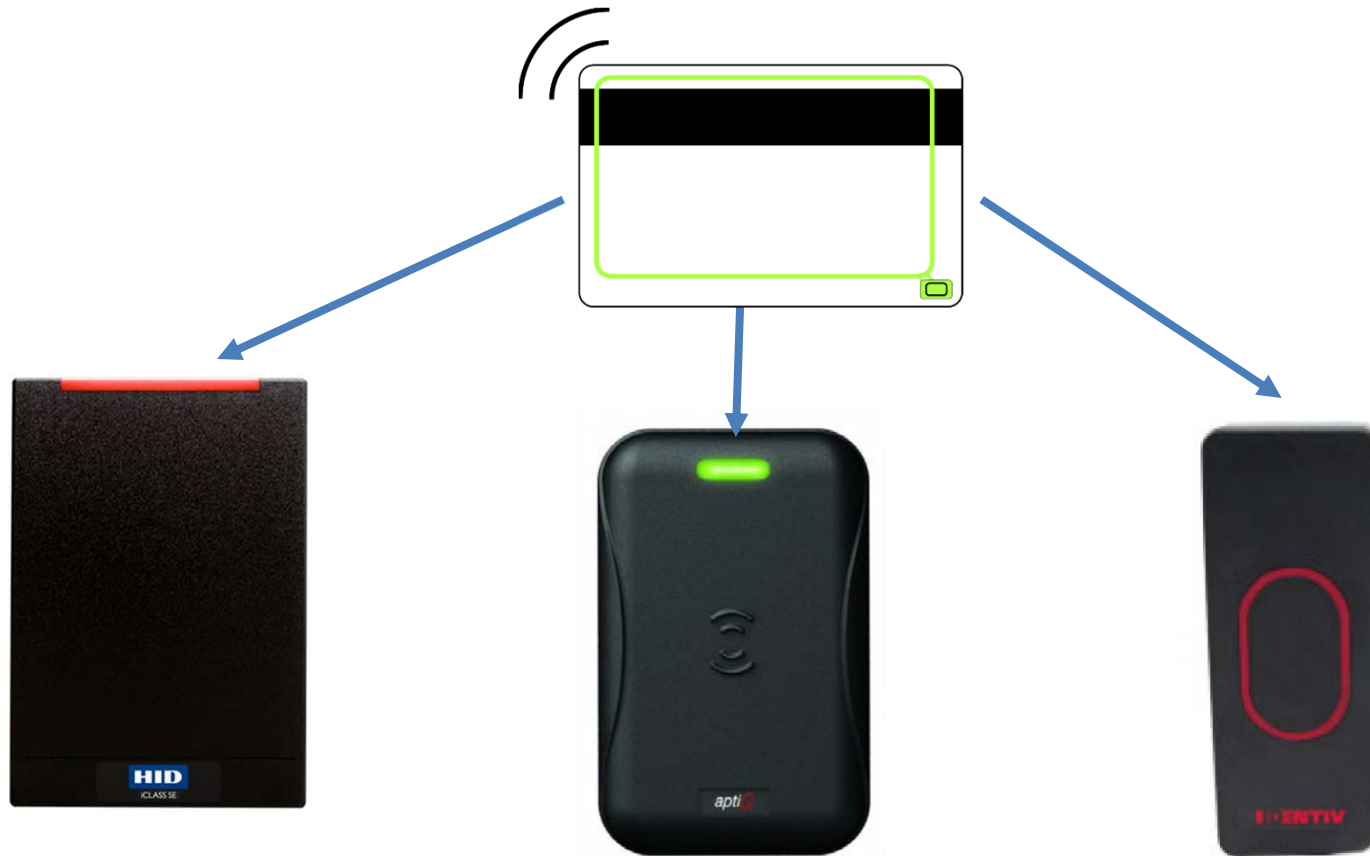
Depends on what the biometric system supports

Most major biometrics have HID readers or support Mifare and DESFire



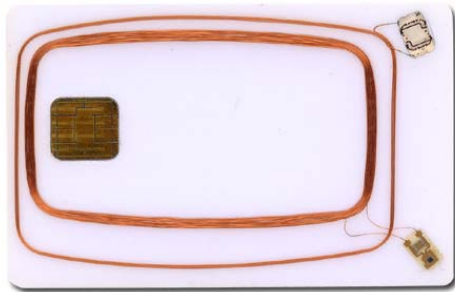
C O L O R I D

# INTEROPERABILITY - PACS READERS

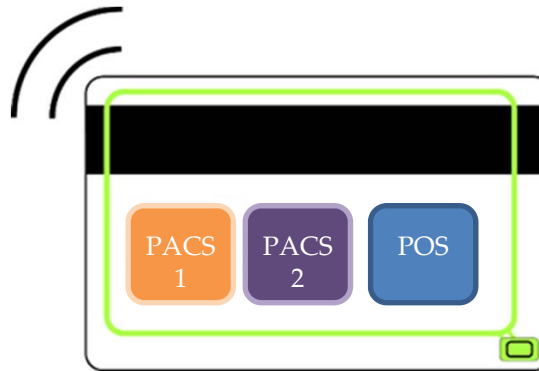


# INTEROPERABILITY - PACS READERS

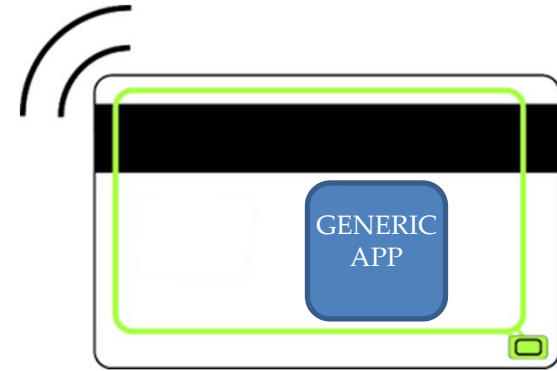
Multiple Chips



Multiple Applications  
on One chip



One Application with  
"Shared Secret"



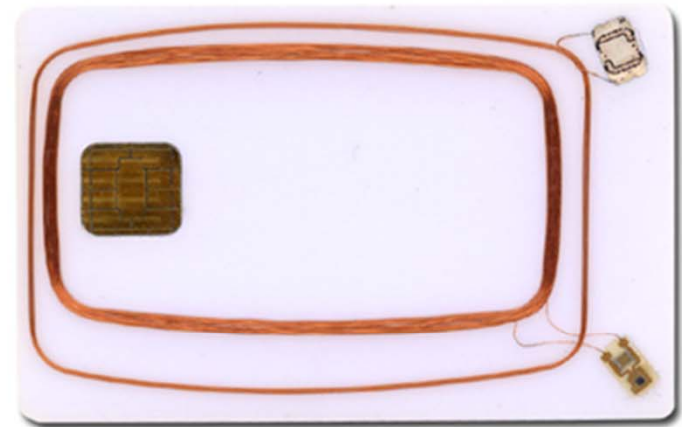
# COLORID MULTIPLE CHIPS

Typically Low Frequency / High Frequency

Sometimes two high frequency chips

Great for Migrating technologies

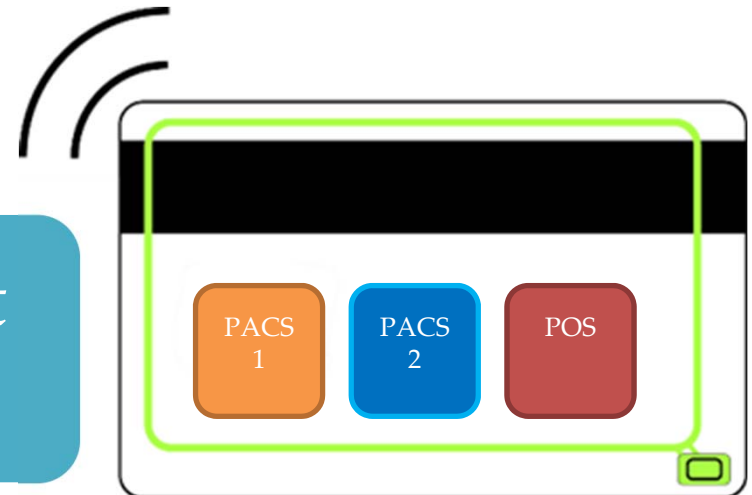
Increased Cost



# COLORID MULTIPLE APPLICATIONS

Encode Apps from different manufacturers to 1 chip

Can be similar cost to multiple chips



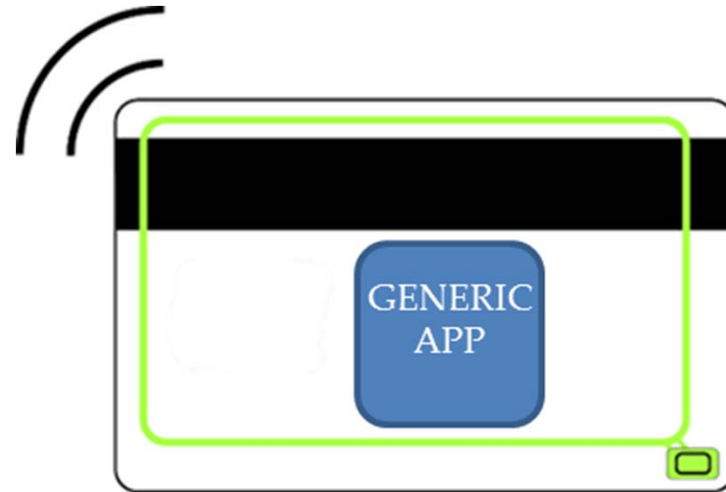
# GENERIC CUSTOM APPLICATION

Requires Custom  
Keys

Custom or “Generic”  
application

Potentially lower cost  
cards

Great in Theory, very  
difficult in practice



C O L O R I D  
**CUSTOM KEYS - FREEDOM**



[WWW.COLORID.COM](http://WWW.COLORID.COM)

© 2018 -- IDENTITY ROADMAP -- ColorID, LLC



C O L O R I D

## CUSTOM KEYS - PROS

Increased Security

No Chance of other cards  
working on your campus

Ability to encode your own  
cards?

Freedom from Proprietary  
Systems?



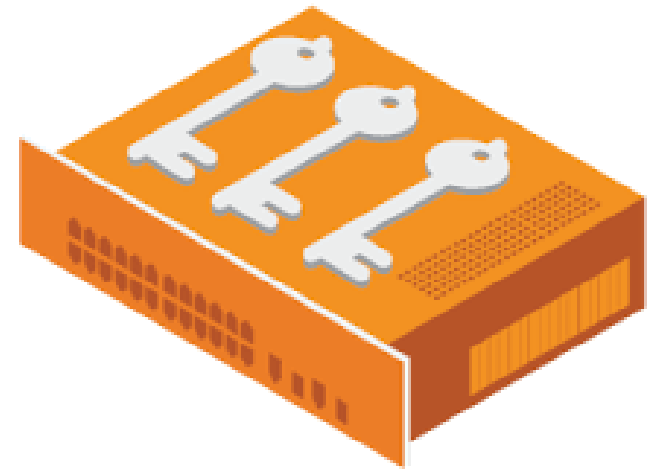
## CUSTOM KEYS - CONS

Key Management – HSM, SAM, Vault,  
Password protected File?

Limit number of people with access

Liability

Consider using manufacturer  
program, but less control



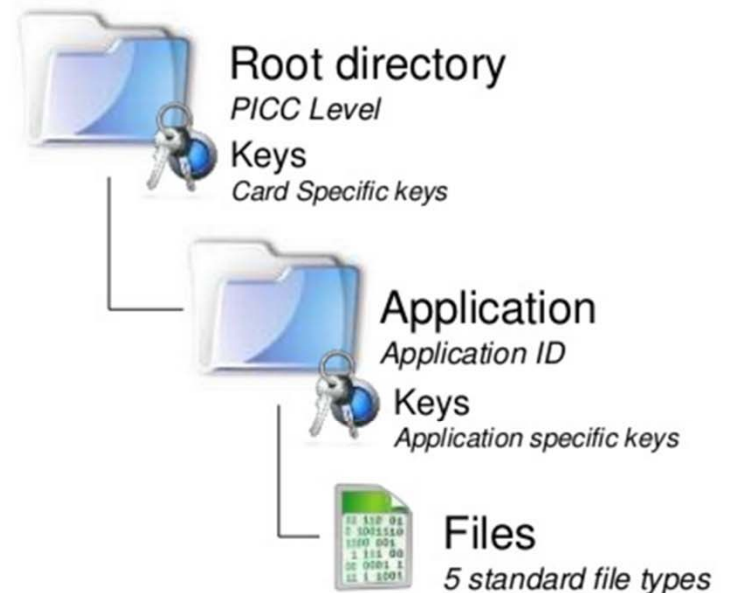
# MORE THAN JUST KEYS – EX) DESFIRE

Application ID (AID)

File Structure (Up to 32 files and 14 keys per application)

Key Diversification (AV1, AV2, NIST, Other)

Most are PROPRIETARY to Manufacturer



# CONTACTLESS CARDS

3<sup>rd</sup> Generation: Mifare DESFire EV2, SEOS

# COLORID DESFire EV2

## DESFire EV2

- Released 2016, still slow adoption
- Can be backwards compatible with EV1
- Increased Read Range and Speed
- New Features
  - Derived Master Keys
  - Key Rolling

MISMART  
APP

Derived master  
keys for secure  
application  
deployment



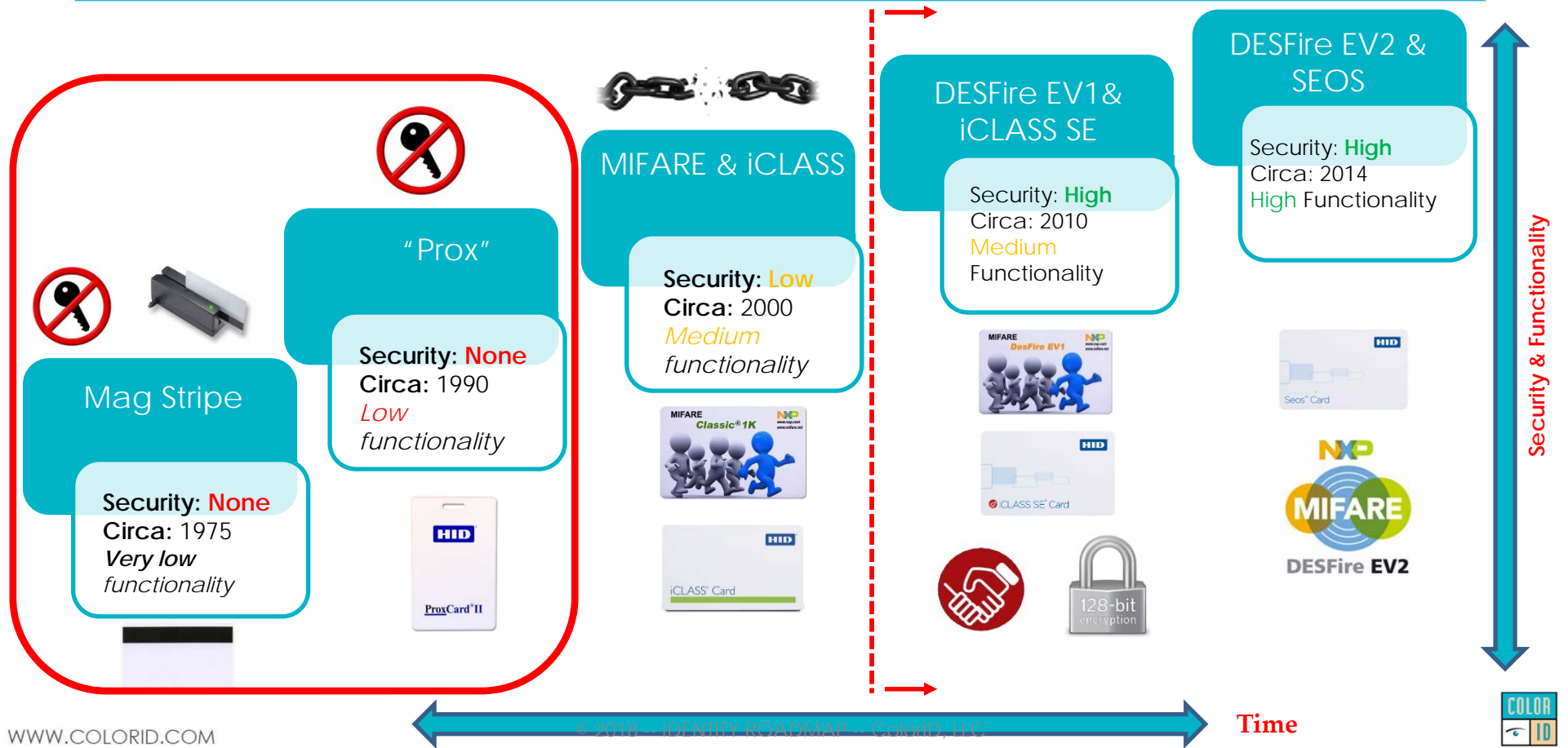
# HID SEOS

## HID SEOS

- Standards Based Cryptography
- Micro-Processor Card
- Available for many device platforms
- Built-in OTP Engine
- Seos Vault on Card
- Software Based – Can be upgraded to combat future security threats



# COLORID CARD SECURITY LEVELS



# CONTACT SMART CARDS

High Security Applications

# COLORID CONTACT SMART CARDS

## Contact Chips

- Very High Security – PKI (Public Key Infrastructure)
- Cryptographic Processor – X.509 Certificates
- PIV, CAC – Federal Bridge
- Mostly Used for LACS
- Slow at the Door for PACS – FIPS 201
- EMV



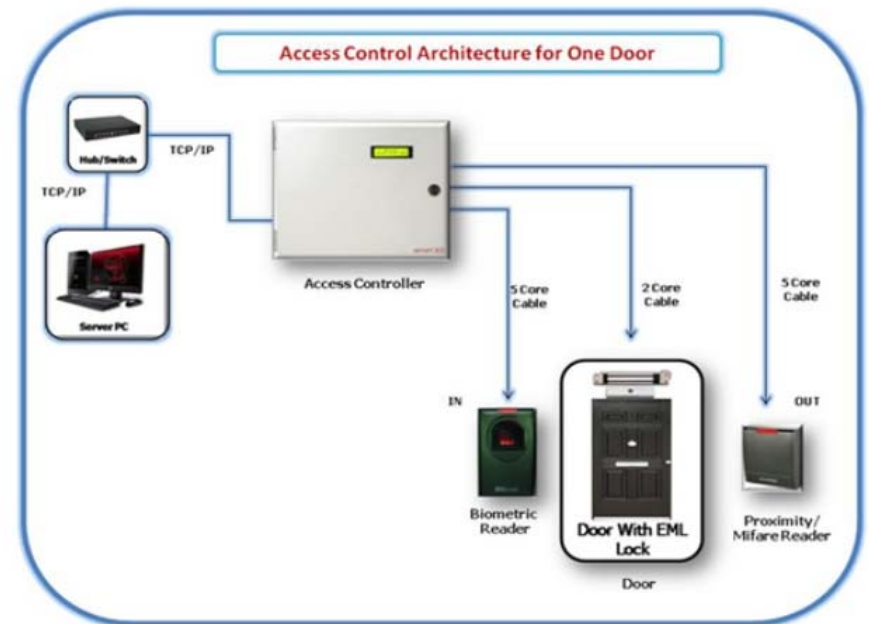
# ACCESS CONTROL

Security Standards in Physical Access

# COLORID PACS BASICS

## PACS Basics

- Readers are “dumb” – just pass Binary Data to Panel
- Mutual Authentication between Card & Reader – “handshake”
- Readers Decrypt Data
- Data sent to Panel
- Panel & Software Parse Data
- Weakest link is highest security level

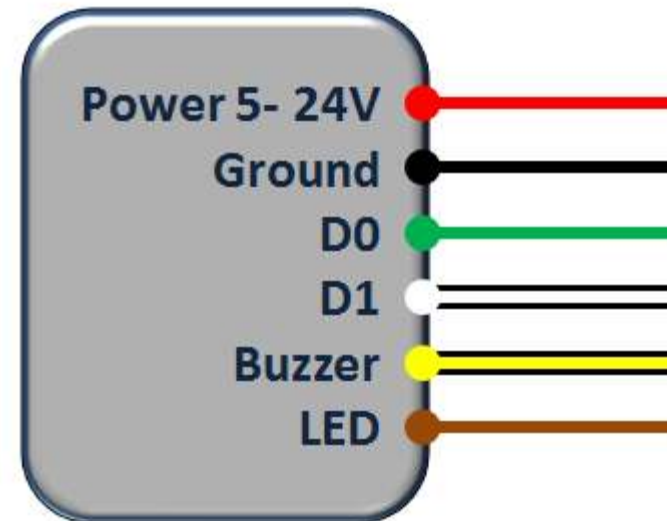


# ACCESS WIRING PROTOCOLS

## Wiring Protocols

- Wiegand – 0/1
- Clock & Data
- RS485
- OSDP

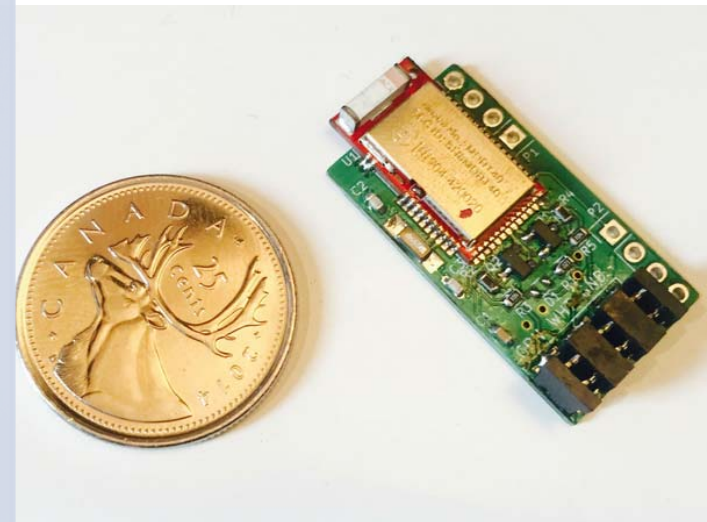
### Standard Wiegand Wiring



# COLORID WIEGAND SNIFFING

BLEKey - [hackerwarehouse.com](http://hackerwarehouse.com)

- “BLEKey is a Bluetooth Low Energy (BLE) enabled tap for the Wiegand protocol, which is the most widespread protocol for proximity card reader systems. BLEKey can be installed in a reader to passively sniff Wiegand data, and can emulate cards on that reader. All data can be offloaded to a phone with BLE support”



C O L O R I D

# FUTURE PACS COMMUNICATION

## OSDP - Open Supervised Device Protocol

- Access Control Standard developed by SIA
- Designed for Interoperability among PACS
- Fully Encrypted Communication
- Centralized Management for Upgrades and Configuration



C O L O R I D

THANK YOU

