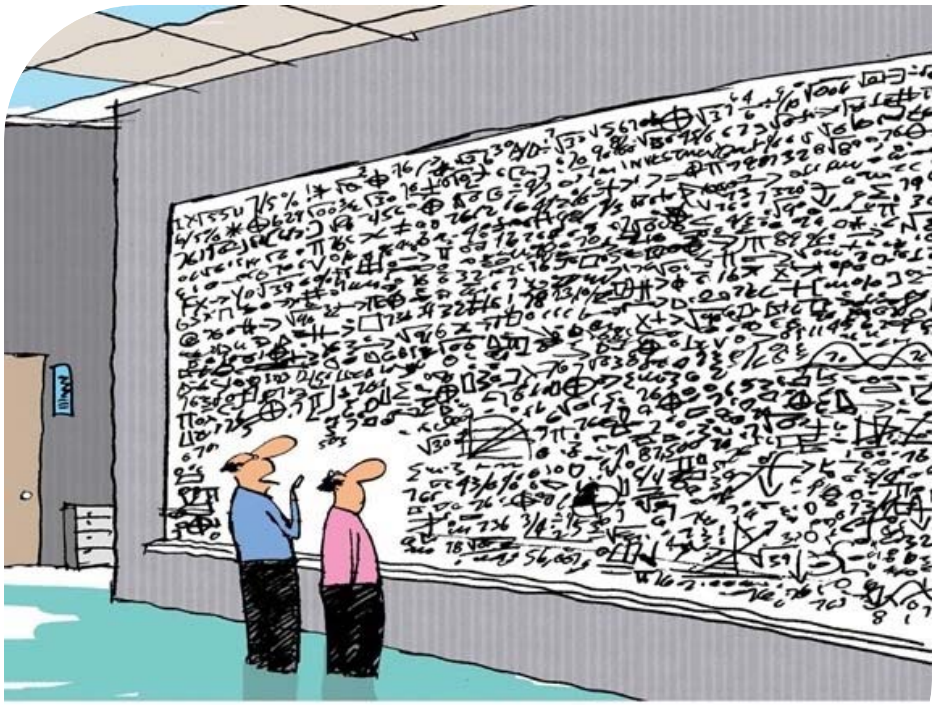
AN INTRODUCTION TO CARD TECHNOLOGY

Fundamentals of Card Technology



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

LEGACY CARD TECHNOLOGIES

Magnetic Stripes, Barcodes, Prox

C O L O R I D

LEGACY ID CARDS

Barcode

- Auto Identification
- Easily Copied
- Printed on any card

Magstripe

- 1, 2, or 3 Tracks
- Normally encoded in printer
- Cards can have 2 mag stripes
- No Security
- Legacy Systems

Visual Security

- ID Photo
- Printed Numbers
- Holograms, UV Inks, Foils
- Logos

C O L O R I D

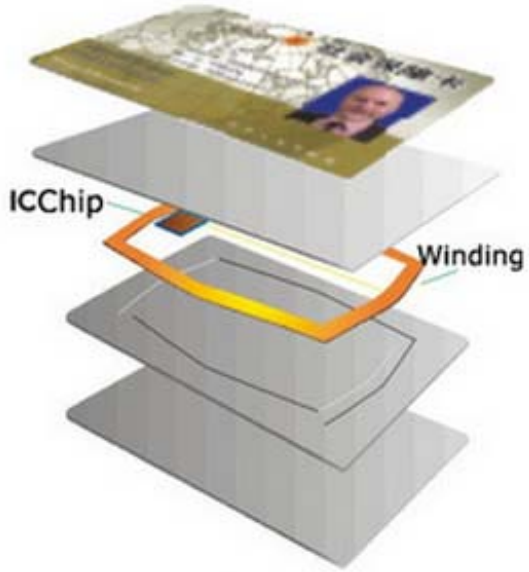
RFID CARDS

RFID

R.adio **F.**requency **I.D.**entification

Three primary frequency ranges:

Low Frequency	Prox – 125 KHz	
High Frequency	Contactless Smart Card – 13.56 MHz	
Ultra High Frequency	UHF, RFID, EPC Gen II	Seldom used for cards



C O L O R I D

PROX CONTEMPORARIES

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

CONTACTLESS CARDS

Previous Generations: Mifare Classic, iClass, DESFire, HID SE

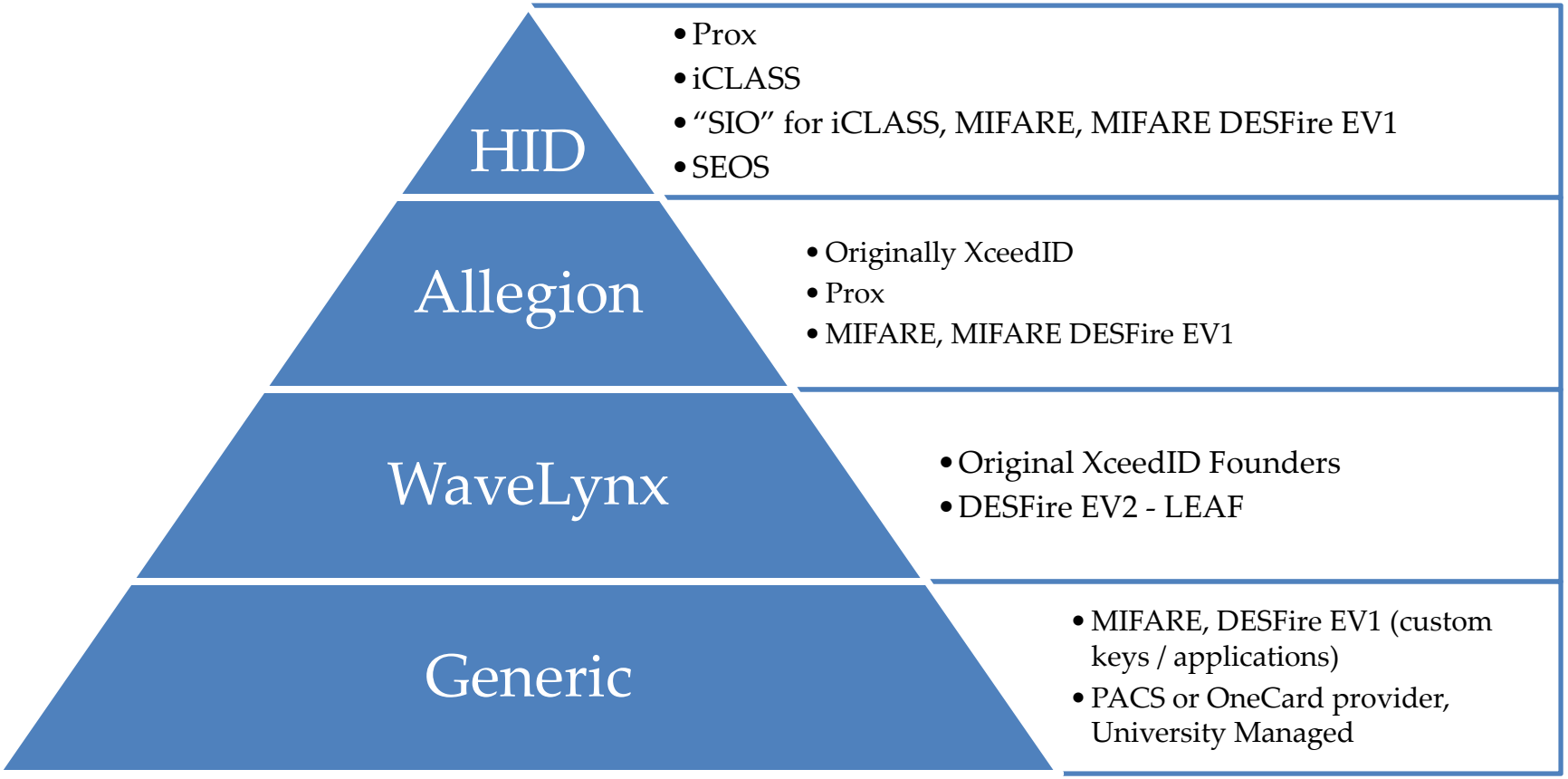
C O L O R I D

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

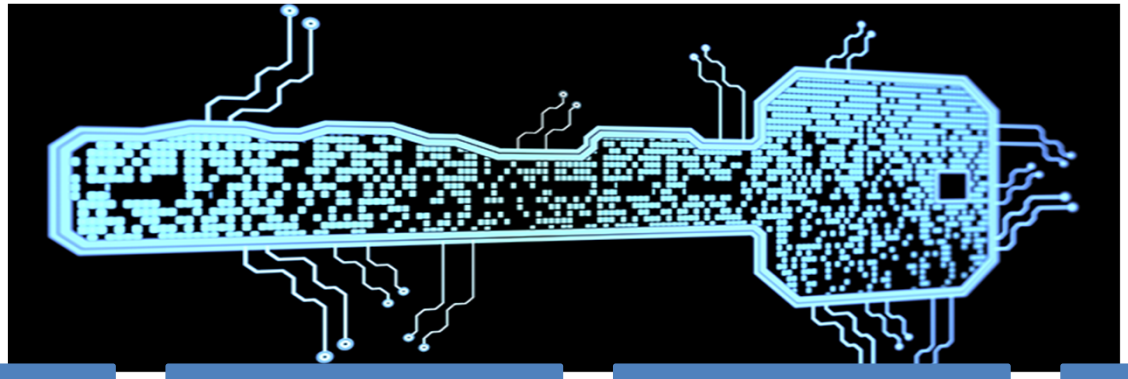
C O L O R I D

CONTACTLESS CARD PROVIDERS



C O L O R I D

CARD DATA SECURITY



Card data security relies on encryption	Encryption keys or keysets	Secure readers and cards typically from same manufacturer	Most contactless card data is static
• Turns data into unrecognizable form • Common Algorithms: • Crypto1 • DES • 3DES • AES	• Card data encrypted with the key • Reader knows the key and can decrypt data • Mutual authentication between card & reader • Custom keys available	• Reader holds the keys and application information for the cards it reads • HID → HID • Allegion → Allegion • Etc.	• Must be encrypted at rest and in transit • Original transit apps used value stored on card

C O L O R I D

CONTACTLESS CARD DATA

Serial Number / UID	Secure Data	Additional applications
• ISO 14443 • ISO 15693 • Card Serial Number (CSN/UID) • Not Encrypted	• Typically PACS data 26-78 bits • Parsed into Facility Code, ID, other • Managed Formats (Corp 1000, U1000, CardTrax)	• Any type of data required • Many use cases

1ST GENERATION CONTACTLESS

Mifare Classic

- NXP (formerly Philips Electronics)
- Crypto 1 Algorithm
- Poor Random number generation
- Most hotels and transit systems
- Easily Cloned

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

2ND GENERATION CONTACTLESS

Mifare DESFire EV1

- 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

HID SIO

Secure Identity Object

- SIO Data can be anything
- Can be preprogrammed by HID
- AES encryption, digital signature, bound to device
- SIO read at door by HID SE readers
- iClass SE, DESFire SE, Mifare SE

CONTACTLESS CARDS

Latest Technologies: Mifare DESFire EV2, SEOS

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

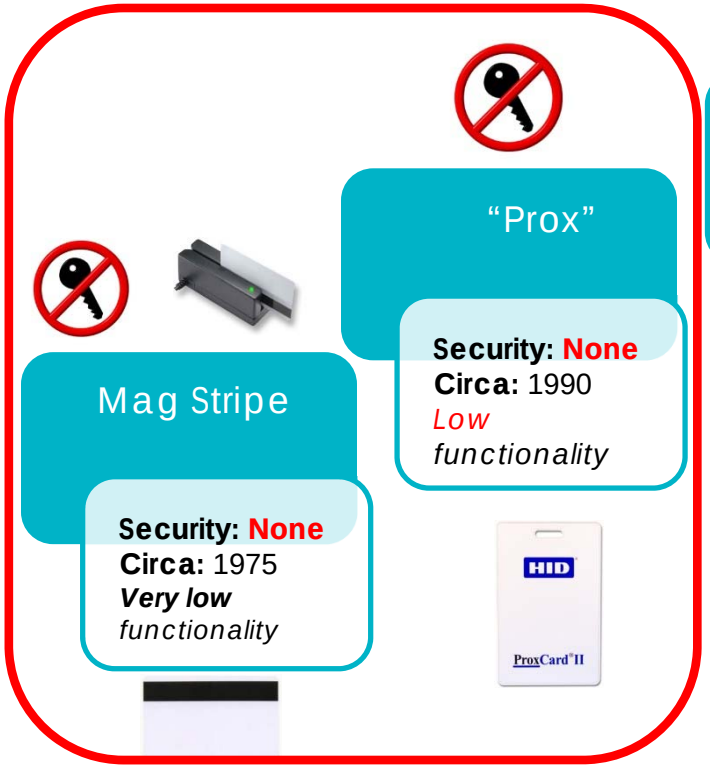
HID SEOS

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

C O L O R I D

CARD SECURITY LEVELS



Mag Stripe

Security: None
Circa: 1975
Very low
functionality

"Prox"

Security: None
Circa: 1990
Low
functionality

MIFARE & iCLASS

Security: Low
Circa: 2000
Medium
functionality

DESFire EV1& iCLASS SE

Security: **High**
Circa: 2010
Medium
Functionality

DESFire EV2 & SEOS

Security: **High**
Circa: 2014
High Functionality

Security & Functionality

Time

CONTACTLESS CARD APPLICATIONS

What can my card do?

C O L O R I D

CARD APPLICATIONS

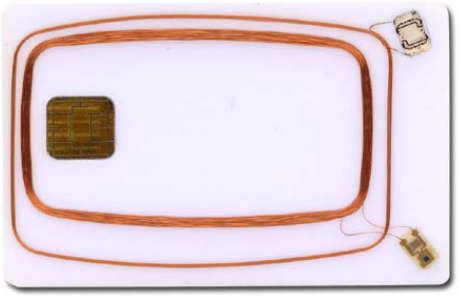
- Contactless Cards can store many applications
- Similar in concept to apps on a smartphone

Transit	Biometrics	Logical Access
• Separate application – typically for NXP cards • Sometimes read UID only	• Depends on what system supports • Most major biometrics have HID readers or support Mifare and DESFire	• OTP for SEOS • USB Reader with 2FA Software

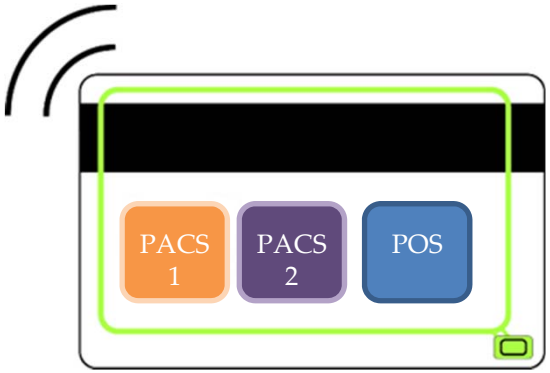
C O L O R I D

INTEROPERABILITY - CARD READERS

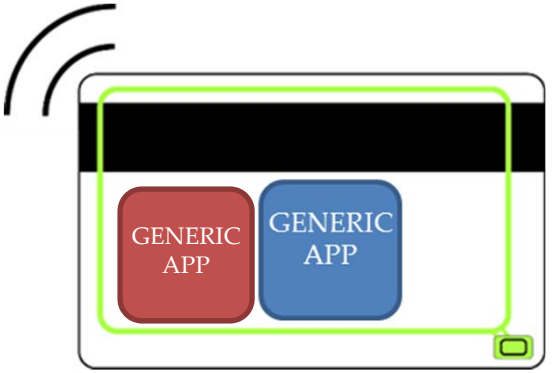
Multiple Chips



Multiple Applications on One chip

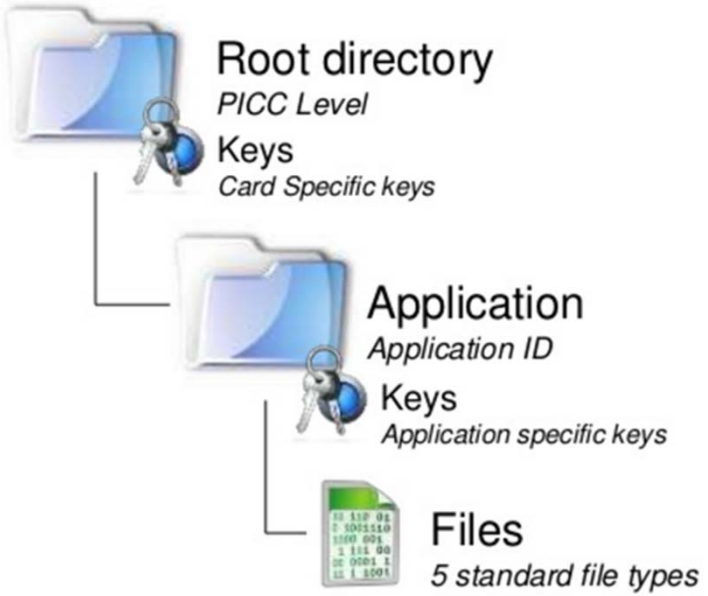


One Application with "Shared Secret"



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



C O L O R I D

CUSTOM KEYS - FREEDOM

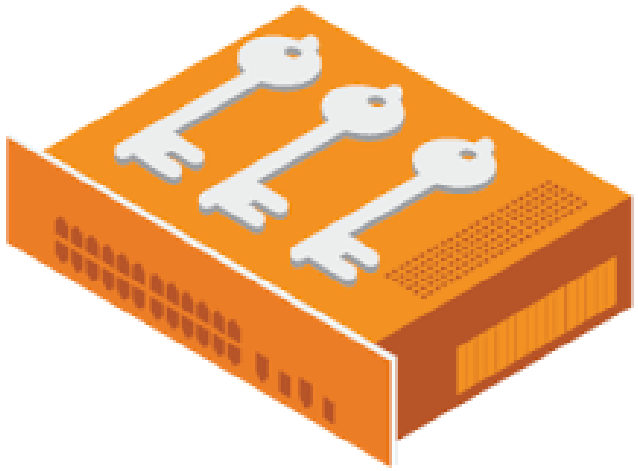
C O L O R I D

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



ACCESS CONTROL

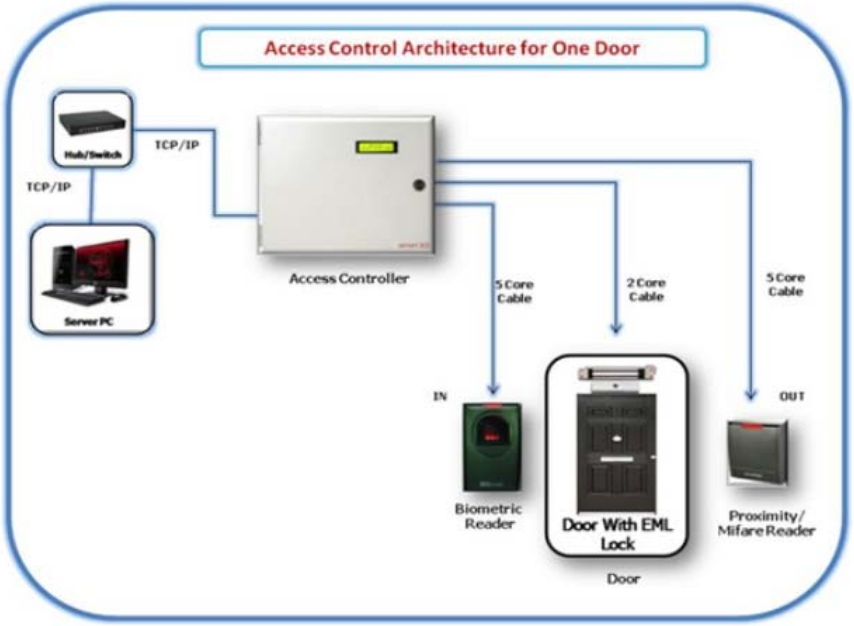
Security Standards in Physical Access

C O L O R I D

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

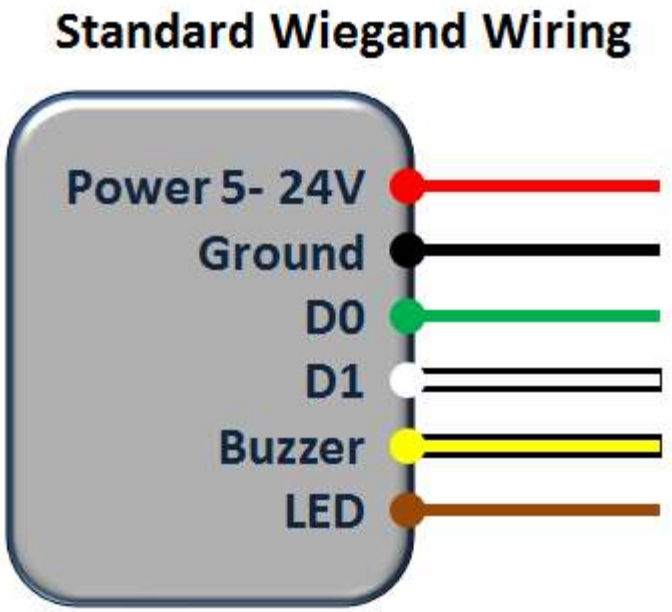


C O L O R I D

ACCESS WIRING PROTOCOLS

Wiring Protocols

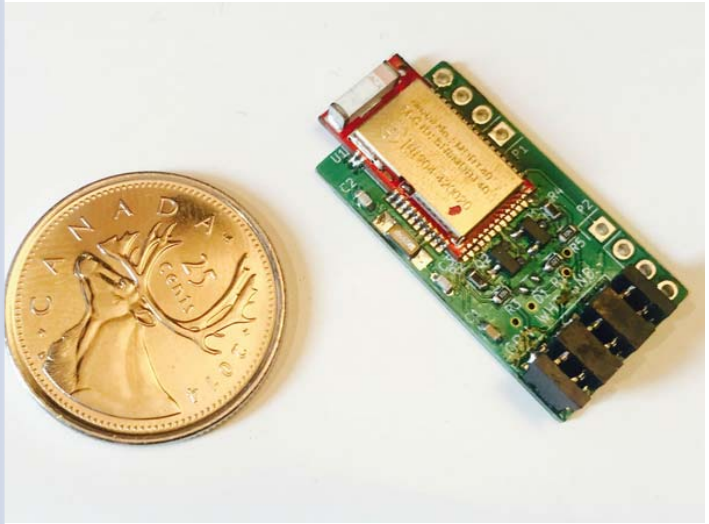
- Wiegand – 0/1
- Clock & Data
- RS485
- OSDP



WIEGAND SNIFFING

BLEKey - **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

THANK YOU