CLEARING UP THE CONFUSION FOR YOUR CREDENTIAL OPTIONS

Todd Brooks
Director of Product Management, ColorID

David Harris
Product Manager, ColorID
Card Technologies
Mobile Credentials
Contactless Card Applications
Migration Process
"...and that, in a nutshell, is how we get to a current, secure student ID..."
Some words you will hear or have heard…

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>The amplitude of a radio frequency. How quickly the wave oscillates over a period of time. Like radio stations (88.1-108 MHz)</td>
</tr>
<tr>
<td>Keys</td>
<td>Much like a key to a house, a digital value that “unlocks” data i.e. the key or password to decrypt</td>
</tr>
<tr>
<td>Data</td>
<td>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.</td>
</tr>
<tr>
<td>Passive</td>
<td>Rather than active. Not powered by a battery (active), but powered by a RF field</td>
</tr>
<tr>
<td>SAM</td>
<td>Secure Access Module - a piece of hardware, a chip, that serves as a vault.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Data security. The act of creating a value that is unintelligible to an unauthorized viewer</td>
</tr>
<tr>
<td>PACS</td>
<td>Physical Access Control System</td>
</tr>
</tbody>
</table>
Card Technology History

- **Generation 1**
  - **Mag Stripe**
  - Security: None
  - Circa: 1975
  - Very low functionality

- **Generation 2**
  - **“Prox”**
  - Security: None
  - Circa: 1990
  - Low functionality

- **Generation 3**
  - **MIFARE & iCLASS**
  - Security: Low
  - Circa: 2000
  - Medium functionality

- **Generation 4**
  - **DESFire & iCLASS SE**
  - Security: High
  - Circa: 2010
  - Medium functionality

- **Generation 5**
  - **Seos**
  - Security: High
  - Circa: 2014
  - High functionality
COLOR ID
PRO X CONTEMPORARIES

Game Boy
Floppy Disk
Windows 95
Cassette Tape
Netscape

WWW.COLORID.COM
• So, why should I consider migrating from Prox. Well.....
COLORID

VULNERABILITY OF PROX

Long-Range In A Briefcase

www.clonemykey.com

$35 on Amazon
MORE APPLICATIONS

• A new level of flexibility that opens new possibilities
• **High-Frequency “smart card”** technology makes it possible to incorporate an increasing number of **physical, logical and extended applications**, including:
  • building access
  • tablet or computer login
  • secure print authentication
  • time-and-attendance
  • cashless vending
  • EV charging
  ...among many more common applications
• With a **truly converged and secure credential**
CARD ENCRYPTION KEYS

What Makes High Frequency Different?

- Encryption – equals “keys”
- **KEYS** are like **PASSWORDS** that lock memory sectors on smart cards
- Once programmed, lock the application with a key
- Types of keys include
  - manufacturer’s standard key
  - custom key unique to the institution
- The reader is the gatekeeper
A NOTE ON SECURITY & ENCRYPTION

- **HID - Secure Identity Object**
  - 13.56 MHz High Frequency
  - Example Cards Used: HID iCLASS SE, Seos,
    - iCLASS SE, multiCLASS SE
  - High level of encryption (SIO) – Hash, AES-128, digital sig.

- **NXP – Classic Encryption**
  - DESFire EV1 credentials primarily use Advanced Encryption Standard (AES), available in 64 bit, 128 bit, and 256 bit levels of length
  - Diversified with the static unique ID (UID, CSN) of the card’s chip.
  - To date, this remains an uncompromised encryption algorithm
  - Predecessors have e.g. Data Encryption Standard (DES) and Three-key Data Encryption Standard (3DES).
  - Keys typically controlled by manufacturer(s)
THE KEYS NEED TO MATCH!

Blackboard → Blackboard
Allegation → Allegion
HID → HID
Custom Keys → ∞
EMERGING TECHNOLOGY

Mobile Devices
WHERE IS ACCESS CONTROL HEADED?

- Mobile access
  - Handhelds
  - Barcodes
  - NFC vs BLE
  - Geo location
MOBILE ACCESS

- Leverages devices students already have
- Reduce lines at card offices
- Reduction in consumable costs
- Can be integrated with non-door control systems e.g. cashless vending
- Cloud-based means minimal local resources
- When device is secured with PIN and/or biometrics, security is increased
- Typically requires minimal, easy retrofit or replacement of all reader

Why consider mobile access?
– In many cases, mobile credentials can be more expensive than a traditional card
– Mobile credential typically is a complimentary credential, not a replacement
– Dead battery means no entry
– Retro-fitting hardware can mean limiting where (and who) can use the solution - $$
– Diverse phone ecosystem can create interoperability issues
– NFC vs BLE
• **HID Mobile Access**
  - Powered by Seos
  - NFC or BLE technology - Long range capabilities and device flexibility
  - Provisioned through web portal or access control software integration - email
  - Secured with SIO

• **aptiQ Mobile**
  - NFC communication
  - Requires sleeves for non-Android devices
  - Provisioned through web portal or access control software integration - email
CONTACTLESS CARD APPLICATIONS

What can my card do?
• Contactless Cards can store many applications
• Similar in concept to apps on a smartphone
High Frequency cards have UID for interoperability

PACS applications from card manufacturer

Similar to PC

- Blocks, Sectors
- Books, Pages
- Applications, Files
Transit

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

Depends on what the biometric system supports

Most major biometrics have HID readers or support Mifare and DESFire
INTEROPERABILITY - PACS READERS
INTEROOPERABILITY - PACS READERS

Multiple Chips

Multiple Applications on One chip

One Application with "Shared Secret"
MULTIPLE CHIPS

Typically Low Frequency / High Frequency

Sometimes two high frequency chips

Great for Migrating technologies

Increased Cost
Encode Apps from different manufacturers to 1 chip

Can be similar cost to multiple chips
Desktop or Fargo Printer

HID or custom applications

HID or Non-HID cards
Requires Custom Keys

Custom or “Generic” application

Potentially lower cost cards

Great in Theory, very difficult in practice
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 MFG program, but less control
DESFIRE EV1 - MORE THAN JUST KEYS

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
CARD APPLICATION TAKEAWAYS

Somewhat complicated technology in contactless cards

Determine most important factors for your credential

TEST! TEST! TEST!
MIGRATION PROCESS

How do we make this happen?
NORMAL CAMPUS COLLABORATION?
KEY STAKEHOLDER INVOLVEMENT

• Meetings with departments
• Vendor presentations
• High level personnel
EVERYONE’S ON THE BUS, NOW WHAT?
KEY TECHNOLOGY DRIVERS

Residence Hall Locks

Schlage AD/NDE Locks
Allegion

Assa Abloy (Sargent, Persona)
HID

© 2017, ColorID, LLC
Mobile Options
**KEY TECHNOLOGY DRIVERS**

**Integrator Options**
- POS / OneCard Vendor Support
- Physical Access Support
- Is vendor support required?

**Other Application Support**
- Transit
- Events
- Local Companies (Vending, Movies, etc)
- Biometrics
MIGRATION PATHS

Dual Technology Cards
- More expensive cards
- Slower reader rollout

Multi-Technology Readers
- Keep existing cards
- Upgrade all readers before changing card technology
- Delayed use of newest technology

Re-Card Entire Campus
- Quickly provide a solution to entire student/staff population

Gradual Roll-out
- Provide new cards to certain populations
- Ex) Freshman class, Staff

Cost Analysis
Campus Dependent

© 2017, ColorID, LLC
Collaborate with other departments on campus

Use Technology Drivers to determine the correct credentials for your campus

Develop migration strategy for moving forward with selected technology

Find a partner to help you navigate this process
THANK YOU

Todd Brooks
todd.brooks@colorid.com

David Harris
david.harris@colorid.com