Cards: What they do and how they do it

Introduction: The NACCU Technology Committee is presenting this Card Technology 101 document to discuss the most common questions we receive on the various technologies associated with operation of a Campus Card service. This will include communication between cardholder devices (cards, wearables, phones) and reader devices (access control readers, point-of-sale (POS) readers, other readers), *as well as a brief overview of identity management principles relative to the Campus Card*. The committee is also releasing an evaluation of the most common card printers.

The Physical Card

There are two common types of card – passive and active. A passive card has physical media, either magnetic or copper, on or in the card itself. There are a variety of physical presentations of a passive card with varying costs and durability. Most common sizes are CR80 (3.375 " x 2.125") most often used for university identification cards and CR100 (2.63" x 3.88") most often used as conference badges or for events. Active cards are generally 3.625" x 2.65" x 0.30" with the added height measurement reflecting the shell that is enclosing the battery and technology.

Cards should not be hole-punched to prevent damaging the copper wire antenna in the card (see photo in the physical media section). They can be ordered with a punch, as shown below with the clamshell card. Clamshell style are more durable cards, a similar hole ordered in PVC or composite cards tends to break over time.

Along with cards comes the task of carrying or transporting them. Some folks will stick the card in their purse or wallet, others prefer a lanyard and holder. These are often used as opportunities for marketing, with lanyards being ordered in specific colors with printing, generally using a plain plastic holder though they may also be customized. Some schools distribute their cards in a small paper wallet that has a slot for the card and pages to include material on the card program and/or campus. Another common item is the silicone gripper which allows the user to secure the card and use the magstripe without the wear and tear of sliding it in and out of a case or requiring a hole punch in the card.

These are mostly convenience items, though a holder may also provide a security function. For those using proximity cards the card will respond to any reader, even those of a criminal capturing data. Using a SkimSafe holder or other RFID blocking technology can help protect the card when not in use.

When ordering lanyards, consider using a breakaway style for safety. These have a clip at the top that will release if the lanyard is caught up in something or pulled on. While a plain clip or keyring is most common at the end of a lanyard, pull styles allow the user to easily present the card and again may be customized for a marketing opportunity. A NACCU conference is a great place to see all of the options available for cards and holders.

Passive

- **PVC** – The cheapest solution, it is a single layer of plastic. May be ordered customized or printed locally, but will often warp in the printing process due to heat from the printer and the thin plastic. May be ordered with a magnetic stripe (magstripe) for media. These cards should not be hole-punched if using a chip in order to prevent damaging the copper antenna.
- **Composite** – The most common for university use. A combination of PVC and PET plastic and may be ordered in a variety of plastic combinations that will determine price and durability. The most common are either a 60/40 or 70/30 combination to create a durable and long lasting card. May be ordered with a magstripe and/or with embedded 125KHz chips for proximity access (prox) or 13.56MHz chips for smart card access (smartcard). The chips are embedded along with a copper antenna, providing the means for the chip to communicate with readers. The 13.56MHz chip can produce a raised spot in the card which may affect direct to card printing. The chip does not affect retransfer printing. These cards should not be hole-punched if using a chip in order to prevent damaging the copper antenna.
- **Clamshell** – The most sturdy card, composed of an ABS shell it is ordered either as a prox or smart card. It may be customized with pre-printing but most often used blank or with an adhesive PVC overlay. These cards come with a pre-punched hole for a card holder.

Active

- **Cards with a battery** – These are less of a card and more of a contained shell that holds the technology and a battery in a plastic housing. They offer the same technology as card and are generally used for vehicles or applications where the reader and the card are at a distance from each other. The battery provides a signal boost for the technology to reach the reader.

Alternatives to Cards

While cards are the most common device used for access and transactions, wearables are gaining popularity. They don't generally have the flexibility a card does to have multiple technologies and additional data such as cardholder pictures, affiliations, dates, etc. They may be customized but are generally limited to a logo or short, simple text. They are often cheaper and simpler than carrying a card, often available to attach to a keychain or worn on the wrist. For those who attended the 2017 NACCU conference in Orlando, the Disney hotel issued watch style wearables for room access, purchases, photos and other park amenities. The wearable is their new standard for issuing an ID to guests. The newest alternative to cards is the mobile ID, growing in popularity to accommodate a more mobile lifestyle it provides a level of flexibility others alternatives don't. While it has been available for many years, the use of biometrics for readers is gaining acceptance.

- **Fobs** – available either in a keychain or adhesive format they are generally the size of a quarter if round or a USB stick if rectangular. Handy for use with conferees or summer campers they provide an inexpensive alternative to cards for transient populations. There is some concern around use and control of these devices as there is no identification of a photo or name tying them to a specific cardholder.
- **Wearables** – available in a variety of formats they are most common as a plastic version of a watch or bracelet. They can also come as phone cases, luggage tags, etc. Wearables have the use and control concerns. A wearable will generally not have identifying cardholder information such as a photo or name. This reduces the ability to verify the user and makes it easier to commit fraud.

- **Mobile** – still with limited availability the technology exchange is between the reader and the mobile device and may be independent of the system used for access control or transactions. Communication is through either Bluetooth or Near Field Communication (NFC). Similar to other alternatives there are limitations, primarily vendor related. NFC transactions are offered on many phones with the notable exception of the Apple iPhone. The use of either an adhesive card holder or a technology enabled case are suggestions to get around this but are generally not well accepted by users. Bluetooth is offered on almost all phones but requires that your application reader supports Bluetooth. For most readers you will want the communication to be via Bluetooth Low Energy (BLE) to limit the draw on phone batteries. In addition, a mobile device may be used to add a biometric factor for authentication.
- **Biometrics** - these are delivered in a variety of formats. Some using actual biometric data such as a finger or thumb print, or eye scan. More common now are the use of markers, such as a handprint or face scan. Biometric technologies have been less accepted due to the cost and lack of reliability but are becoming more refined and may be in greater use in the future. The infamous use of a gummy bear to replicate a fingerprint is hopefully a thing of the past and there are opportunities available with biometrics that aren't available in cards. For example, using facial recognition to identify tailgaters.

Physical Media on cards

Magnetic stripe

- **Oldest card technology using the same physical media as cassette tapes.** The magnetic surface is adhered to a card and needs to be ordered as part of the card. The magnetic stripe is located 0.223 inches (5.66 mm) from the edge of the card, and is 0.375 inches (9.52 mm) wide. The magnetic stripe contains three tracks, each 0.110 inches (2.79 mm) wide. It is easily compromised with reader inserts that collect data. The most common technology for transactions and was

the most common for access control until the introduction of contactless technology. Many universities are still using magstripe as their primary card technology.

- **Physical components are tracks and coercivity.**
  - There are three standard magstripe tracks commonly referred to as Track One, Two, and Three. A track is determined by its width and distance from the long edge a card. As an example track two is sandwiched between tracks one and three on a half inch width magnetic stripe, there is no hard physical barrier. Track two read/write heads of encoders and readers are positioned at the specific distance from the edge of the card stock.
    - Track One – commonly encoded as IATA and is 7 bit alphanumeric encoding. If you swipe a card and it displays your name on a receipt or screen it most likely read this off your card.
    - Track Two – Commonly encoded for banking with 5 bit numeric encoding.
    - Track Three – Often referred to as the junk track, it contains any additional custom information.
  - Coercivity is the resistance of a magnetic field to changes. It is measured in Orsteads and refers to the strength of the magstripe. The stronger the coercivity the more durable the stripe. The two primary stripes on cards are Low Coercivity (LoCo) and High Coercivity (HiCo). LoCo is commonly 300 Orstead and HiCo is generally 2750 to 4000 Orstead. Looking at the magstripe light brown is LoCo while very dark brown or black is HiCo. Very few LoCo cards are used in education markets as it has a tendency to demagnetize or lose data easily. It has been used more for hotel cards or similar low use applications. Universities tends to use HiCo cards for the durability of the stripe to support many uses. It is also used on credit cards and similar high use cards.

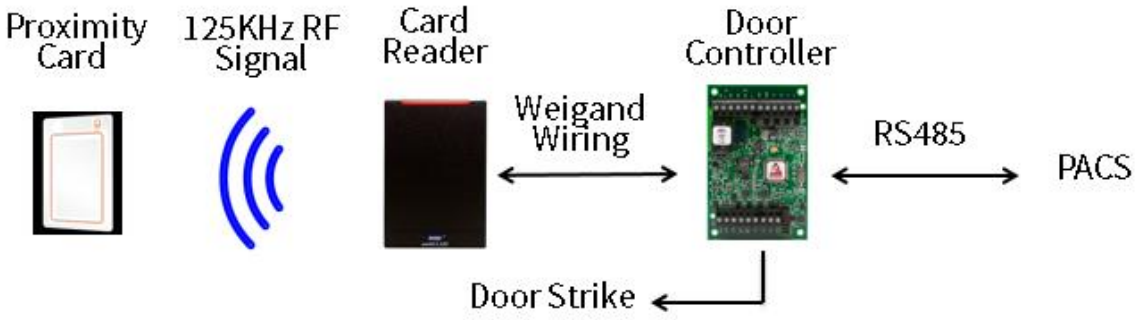
- **Barcode**
  - Barcodes are ubiquitous in modern society. They are used throughout modern daily life so often we are unaware that we may be using them. You will find them on virtually all packaged food products, FedEx, UPS and postal packages. Advertising, web sites and for universities most importantly we use them on identification cards. it is optical machine-readable data. Read by an electronic eye reader set to recognize barcode format, there is no wear and tear on the card. Readers must be ordered to match the formats of code being read. Bar codes come in a myriad of forms some look like stripes, or squares, or circles some are not just black and white but they also come in color they are more commonly referred to as either linear or Matrix/2D. Common bar codes you may

come across are UPC (Universal Product Code) , and QR codes . In this text I am going to discuss the linear bar codes which are the most common for uses with ID cards.

- Many different linear bar code formats exist some like “UPC” can only represent numeric information where as a “3 of 9” can encode 0-9, A-Z and special characters.
- Some linear Bar Code formats
  - Code 128
  - 2 of 5 standard
  - 3 of 9
  - Codeabar
- The reality of a linear bar code is that it is a font just like Times Roman or more apt Wing Dings. So using a my word processor I downloaded a free font and with that I change the font of 12345678 to

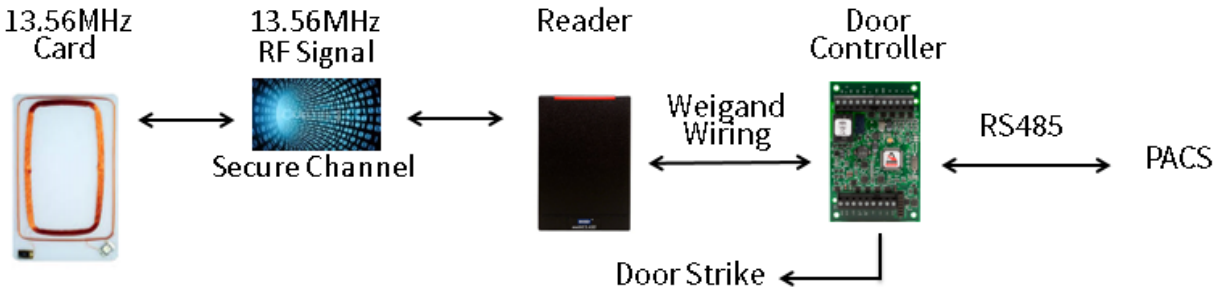
- While in many cases we talk about the security of Magnetic stripes and how technology has been put in place to secure this data PCI and EMV there is little if any discussion on the security of bar codes in the university ecosystem. There is some unfairness comparing to magnetic stripe since magnetic stripes are used for financial transaction and bar codes tend to be used for less secure transactions. Many uses on campuses can be an issue such as checking out library materials, game attendance, and class attendance.
- Pros
  - Easy to Create
  - Read from a distance
  - Simple
  - Cheap (just print ribbon black panel)
- Cons
  - simple to copy and counterfeit
  - Barcode damages easily
  - Zero security
  - No issue code or lost card code
  - Multiple copies will work
  - Take up card real estate
- Linear bar codes on universities are still fairly prolific and while there is some support for the non-contact read vs a magnetic stripe and card wear the overall advantages of the magnetic stripe seem to be superior solution.

- **125KHz Proximity Chip**



  - The most common contactless chip it is embedded in a card with a copper antenna. The antenna responds to any 125KHz signal generated by responding with its programmed information in the clear. The read range is up to 15 inches and may often be read through objects such as a pocket, purse, or wallet. In an active card with a battery this range may be increased to 6 feet.
  - The data stored cannot be manipulated or protected which allows it to be easily compromised. Inexpensive devices (around $20) may be used to read and reproduce the prox chip data.

- **13.56MHz Smart Chip**



  - As the vulnerabilities and ease of compromise for prox chips grew, newer more secure chips were implemented on a new frequency and with computing capability. Smartcard chips are able to hold more data and may even be used to perform authentication or other computing functions. The read range is much shorter, generally only 3 to 4 inches, and will often not perform well through objects. The most secure implementations tend to be proprietary.
  - The data stored may be protected, and allow secure channel communication between card and reader. In most cases this requires that the card and reader are from the same manufacturer – an HID card with an HID reader, an Allegion

card with an Allegion reader, etc. A card will function with another vendor's reader, but you won't get the same level of protection. Generally you will be using the secure technology with the matching reader and prox technology with the non-matching reader. This may also mean ordering a multi-tech card along with your multi-tech readers. You could also choose to program the secure sector of your card to allow a more open communication with an alternate vendor technology.

- NXP makes the NFC technology linked to the NFC chip. This comes in multiple flavors, such as MiFare, MiFare DESFire, or FeliCa. MiFare was the initial implementation of NFC and is the standard for transportation technology. It has been publicly compromised, however, it is so broadly deployed that the move to more secure technology for buses, trains, etc., is largely cost prohibitive. The initial compromised led to the development of the DESFire standard in either EV1 or soon EV2 format. This is a more is a secure implementation and designed as more of an open standard but is still owned by NXP. As an example, the Allegion Aptiq offering is based on DESFire. The biggest drawback to NFC remains the lack of support on Apple iPhone. It does provide added ease of access though has a similar read range to the card.
- Sony makes the Felicity Card (FeliCa) technology which is also linked to the NFC chip. FeliCa is programmed to create a new encryption key each time it is used.
- HID makes the Seos technology. It is their secure standard for readers and cards. If you choose to use Seos you must at some point go through HID for your credentials. One major benefit of Seos is that it may be used with Bluetooth. If you are moving toward a mobile option this is a way to implement that will include the widest variety of devices, including the Apple iPhone. Bluetooth aids the smart card implementation by providing extra distance and ease of access rather than the shorter read range on cards.
- In selecting a credential it is prudent to consider having a custom key from the provider. This means that card 123456 at Location A will be different from 123456 at Location B beyond just the facility code, which is easily determined and compromised. The custom key should be carefully managed and protected, as it is literally the key to your kingdom.

Technology Decisions for a Card Office

Many universities are still magstripe based and are looking to contactless as a future opportunity. The biggest decision is to determine which contactless option to migrate to and how. The choices are generally either prox or smart card, and for the smart card the choice of NFC and/or Bluetooth. Regardless of the choice you make, there will be a migration process including both cards and readers.

Two primary concerns in the new technology decision are cost and security. Choosing to move to prox will be a less expensive implementation but will provide no added security. Prox is easily and publicly compromised so the only benefit will be moving from a contact technology to a contactless technology. You will have less wear and tear, but again, no added security. Moving to a smart card technology will be more expensive for the cost of the cards but will provide a level of security that you can't get with magstripe or prox technologies. If you are taking the time and making the investment in a change a smart card is highly recommended.

For the change you can go big bang and swap all cards and readers at once. For most locations this is not practical as just the timing of this makes it difficult. If you are only changing cards, that may be accomplished fairly easily. If you are changing your readers as well it is difficult to do this on a broad scale quickly enough for a big bang change making it impractical for most campuses.

A more common approach is a combined technology migration where you purchase cards and readers that will accommodate both your existing technology and your future technology. These are often referred to as multi-class cards and readers.

For many this will mean adding a technology to your existing card. For example, if you have a magstripe only card you would begin to order cards with both magstripe and prox, or both magstripe and smart card. If you have a combination of technologies deployed or planned on your campus, you could also go with a card that has magstripe, prox, and smart card together. While the latter provides the most flexibility the more technologies you put on a card the more it will cost. Keep in mind that the more expensive card only needs to be purchased for the migration period. Once the legacy technology has been replaced you don't need to order it anymore. The exception would be if you have different portions of campus using different technologies. For example, your transaction system will remain magstripe while your access control moves to smart card, but you have departments also using prox for other applications. By ordering a multi-class card you retain the access to the current/legacy technology while building in the planning for a future technology.

Once you are ordering multi-class cards you can start to install multi-class readers. For many this will be a magstripe reader attached to a contactless reader as a single device. For some this will be a reader that has multiple contactless technologies, for example Prox, NFC, and BLE in one contactless reader. It will be most common to deploy multi-class readers either on a replacement basis or as a specific project over a defined number of years based on the budget available. You will have cards and devices with multiple technologies available during the migration that may then be programmed more securely once the migration is complete.

As an example, Stanford University chose to go from barcode, magstripe and prox to a Seos solution. Cards with magstripe and prox were already being ordered and the magstripe and barcode was printed on the card. This transitioned to ordering cards that had all these technologies in them. Initially a standard Seos solution was deployed, but was quickly changed

to use a custom key. This meant the first set of Seos cards had to be replaced once the custom key was deployed.

Due to budget constraints, the migration of readers was a three year project. The upside of this is that three years of students, faculty, and staff had the new technology cards by the time the final technology change was ready. In the initial installation all technologies were enabled in the multi-class readers. Once all the readers had been replaced a project to go back and turn off the less secure technologies went forward. A planned replacement of the remaining older cards on campus went forward as well. A mobile solution was also deployed using the secure Seos technology and BLE. The requirement had been to include as much of the campus community as possible which meant including the large contingent of Apple iPhone users in the solution.

As access control moved to Seos, this meant working with departments across the University using other technologies. For transactions this was largely magstripe, and for libraries largely barcode. Efforts are underway to work with those departments to deploy a more secure exchange of information while accommodating the investment in place by the departments.

Implications of Mobile Solutions

There are already mobile applications for registration, classes, etc., and there is a growing tendency among incoming students to expect a fully mobile environment, including their access control and purchase transactions.

Cost is still a major consideration when choosing a mobile solution. Two models, either one time cost for a license or an annual subscription for a license, are still under consideration. The cost of a one-time license is similar to a low cost card, but it is more easily destroyed with either phone upgrades or resets. The subscription costs present an annual cost not currently part of most card office models.

The primary access concern with mobile solutions come from the Athletics, Libraries, and Housing organizations. These are areas with controlled access that may not want a single cardholder to have multiple means of access that would easily allow duplicate use of the facility. While this may be addressed through policy, most universities do not allow sharing ID cards, it is a temptation to avoid.

Another component of allowing mobile solutions is the ability to show a cardholder is a member of the campus community. A Mobile ID that reflects the photo, affiliation, and other pertinent information that would have been on the card is required. The access and transactions do not require this piece but it is necessary to create a fully functional solution.

Other policy and procedure questions come into play once a mobile solution is deployed. Most card offices require a cardholder to come to their office and show government ID to get a replacement card. Once the ID is able to be issued over the air, do you still require the cardholder to come to you? If not how are you verifying the cardholder? If an authenticated email is used to issue the ID it may be enough verification of the cardholder.

Many card offices use the funds generated from replacement cards for a significant portion of their budget. If a card is no longer being issued would the cost for a replacement, and thus the associated revenue, be decreased? You could decrease the cost of a replacement ID by the cost of the physical card and still charge the balance. The challenge may then be the optics of the charge and how you justify it if it is beyond the time spent in labor and overhead. While it would be possible to implement an annual charge in most universities this would not be received well.

Applications and Technology Choices

Selection of a technology will be influenced by the applications in use at a campus. Highlights for common applications are as follows:

- **Blackboard** – offering both access control and transactions Blackboard uses NFC technology. While they are compatible with HID access readers, and so with Bluetooth for access, their transaction readers are proprietary and remain limited to NFC. At this time NFC/DESFire EV1 would be the most secure implementation for a Blackboard school but it would not allow use of Apple iPhone devices for mobile access.
- **CBORD** – offering both access control and transactions CBORD is primarily focused on using a mobile app to communicate with the device. It is also compatible with the HID or Allegion readers, and thus Bluetooth or NFC. In addition, they support an RS 232 connection on the Aero transaction reader which will also allow an external reader connection.
- **Lenel** – offering access control Lenel offers their own Bluetooth reader and is also compatible with either the HID or Allegion readers.