ASSA ABLOY

# Episode Four: Unlocking the Smart Card

The global leader in door opening solutions

*This is an excerpt from Unlocked — an ASSA ABLOY podcast series on campus security. Unlocked explores the security issues and challenges that colleges and universities face as they strive to create a safe and secure learning environment. Visit intelligentopenings.com/unlocked to hear more.*

## How We Got Smart

Before diving into the current credential technologies, it helps to understand where we came from. In 1960, a young engineer from IBM named Forrest Parry invented the magnetic stripe card. Once ubiquitous on campus doors, more reliable and secure technologies are quickly eclipsing the mag stripe.

Mag stripe cards are simple. A card gets swiped in a reader. That reader then reads a sequence of numbers stored on the stripe of that card.

If the number matches what's stored in the access system's database, the door unlocks.

Many campuses still use the mag stripe card for their door access. This is mainly because the cards are inexpensive, the cost to replace the existing swipe readers is high, and other systems aside from security still rely on that technology—namely campus one-card systems that use the card for dining, laundry, vending and other purchases.

Yet, outside of higher education and older hotels, hardly anyone still uses mag stripe cards for door access. In the 90's the access control industry made a wholesale shift from mag stripe to the new, contactless technology called prox—known more officially as "low-frequency proximity".

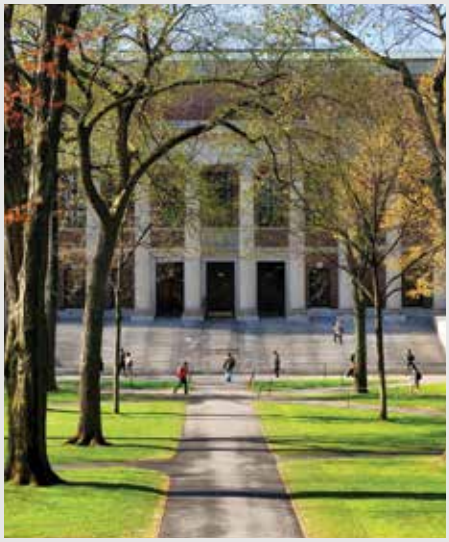
When the prox card came on the scene, everyone was thrilled.

The mag stripe card was cumbersome and inefficient. Not to mention administrators felt the financial sting and maintenance headaches from broken cards and physical wear on the readers. Prox solved these problems. Lower maintenance costs, increased user convenience, and new options for form factors like fobs made the prox card a winner. But the low-frequency proximity technology is not without its limitations.

*Outside of higher education and older hotels, hardly anyone still uses mag stripe cards for door access.*

Like the mag stripe, the prox card is unencrypted and static—making them easy to clone or forge. You also can't encode additional information onto the prox cards, like multiple IDs.

Out of these security limitations and frustrations came the contactless "smart card" as we know it today. The biggest technology difference between smart cards and prox cards is the frequency of the chip inside. Prox cards use a low-frequency 125kHz technology, whereas the new breed of smart cards use a high-frequency 13.56 MHz technology.



Whether installing a new door access system for your campus or upgrading from a legacy system you have a lot of decisions to make.

You first must choose the right access software and locking hardware. You also need to find a knowledgeable and trustworthy integrator to install and service your system. And you need to determine which card technology is right for your campus.

And this last task is not always as easy as it might seem.

A common misunderstanding for campus IT professionals that deal with physical access security is differentiating between the access cards. How do you know which technology is the right one for you?

A lot of technology is packed into the cards. And there are a lot of marketing materials surrounding which cards are best for you. It can be difficult to figure out exactly what your campus needs.

And what you don't.

## Smart Card vs. Prox

Although a massive install base of prox technology exists, the last five years have a seen a transition to smart card technologies. According to Eric Widlitz, vice president of sales at Vanderbilt Industries, he sees no reason not to make the transition.

"You certainly have a gigantic install base of prox technology that you'll continue to support for a long time moving forward," says Widlitz. "But smart card technologies today from a cost perspective are pretty much the same price. And in some cases, may even cost less money than a proximity card."

It's well known that smart cards are a more secure credential than prox. But another advantage that smart cards have over prox is the ability to store and secure other useful information on the card itself.

*"From a cost perspective, today's smart card technologies are pretty much the same price as a proximity card. In some cases, they may even cost less."*

Widlitz explains: "A prox card is kind of like a license plate. It will transmit one ID number to the system and that is all it is capable to do. And it's not secure. On a smart chip, you have multiple containers that you can store different applications in. Each one of those containers is secured. Think about it like a filing cabinet, and you have a key to each one of the drawers on the filing cabinet. There's an encryption key that secures the information on the card for each one of those applications. It can be used for multiple applications where you can't use any of the previous types of technologies for that."

The difference in frequencies between the prox card and the smart card can also affect performance. But not in the way you might think.

Schools that purchase the smart, or contactless, card for the sake of convenience for their students can be surprised to find out the read range is limited on the smart card.

This is because the difference in frequencies on the card can have an impact and effect on the card's read range. You typically get a slight reduction in read range with smart cards. And the read time and the communication time between card and reader is a little bit longer.

"You definitely take a little hit on the convenience side on the speed and read range that you have. But you have the insurance that your information is secure on that card and that people can't take that information off your card," says Widlitz.

This is something to keep in mind when your campus starts discussing the benefits of smart cards. Fortunately, as people get accustomed to longer read times of EMV credit cards they are less prone to notice the slight increase of speed on the contactless cards over the prox.

To recap, here are three reasons to choose a contactless smart card over a prox card. Or why you might consider upgrading from an existing prox card installation:

1. Contactless smart cards are safer. They can't be copied, or "skimmed" in the way prox cards can.
2. They can cost the same—or in some cases—cost less than prox.
3. They can store additional data and be used for other applications, like transit systems.

"There is absolutely no good reason today—starting with a new, fresh install—why you would ever put in proximity technology or put in mag stripe technology," says Widlitz.

"You should always think about moving forward with some sort of smart card technology."

## Smart "One Cards"

A source of confusion unique to higher ed when it comes to smart cards, is the term itself "smart card". While smart card is used universally in other verticals of the physical security industry, in higher ed we tend to refer to them as contactless cards.

Why? Well here's a little history lesson. A bunch of years ago smart cards became popular on a handful of large universities for student purchases like vending and laundry, and for meal plans. What we now call One Card systems. These smart cards were of the contact chip variety. The eventual problem with them was the money was stored "offline" on purses on the card. As networked, "online" systems gained in popularity these smart card systems became irrelevant. Just about all those smart card systems have been ripped out and replaced on the campuses who used them.

And because of that experience, the term "smart card" when talking to campus folks who also deal with the one card, payment side of the credential has left a bad taste in their mouth. That is why most vendors dealing with the payment side refer to the newer technology cards almost exclusively as contactless.

So you see how confusion can arise when a one card vendor calls them contactless, and a security vendor calls the same card a smart card.

Most people in the security industry will use the term smart card to encompass pretty much all types of contactless cards that aren't prox.

> "If you are considering purchasing a smart card and only plan to use the serial number, it's no different than using a prox card."

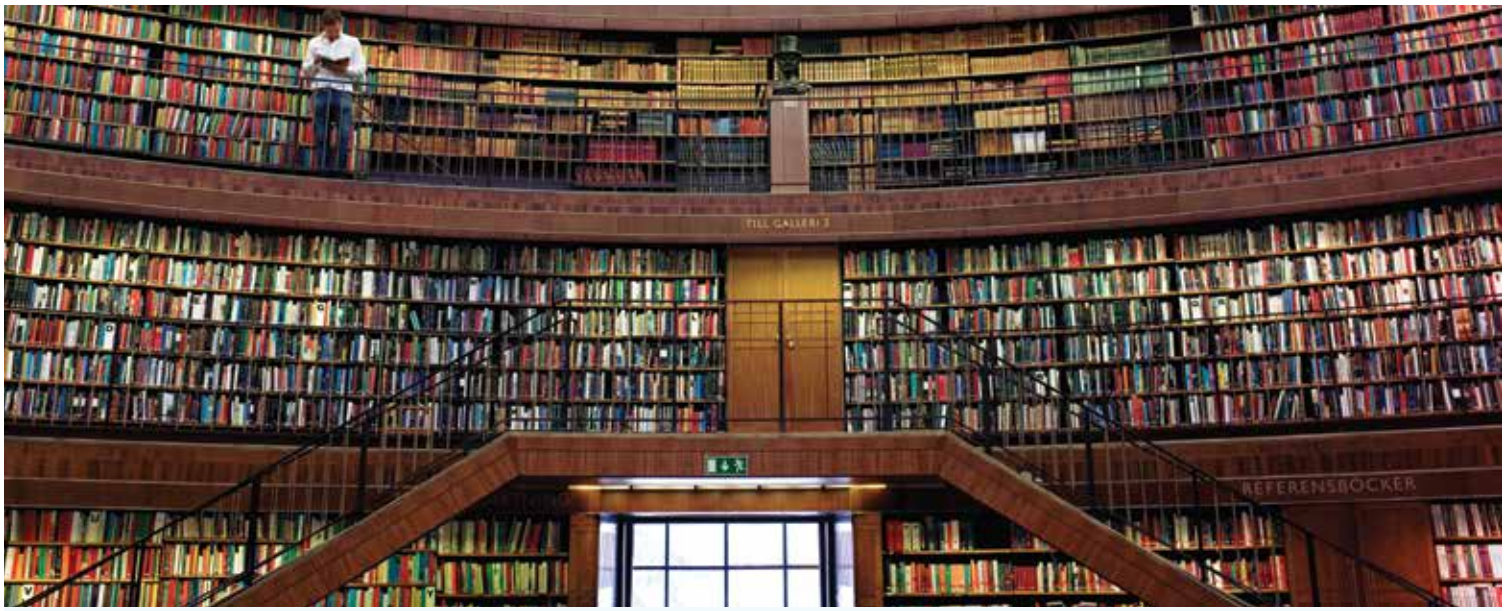
## Trust in a Handshake

For colleges and universities, one of the biggest benefits of smart cards is that they are more secure than the prox card. This is because of something called mutual authentication.

According to Widlitz, mutual authentication works like this: "In the simplest of terms, a reader will boot up a chip, start a chip, they'll start talking to each other. And they do a kind of handshake to authenticate each other. And if they authenticate each other, then the smart card will start releasing the information that's being asked for."

So, the card reader performs a couple tests that the smart card needs to go through to make sure it's communicating with the right type of card. And if they have that correct handshake together then the process will continue, and they will continue to talk to each other. If that handshake or something goes wrong at that initial communication, then the card and reader will stop communicating and the door will remain locked.

Without delving into the details of the cryptographic authentication, it's important to know that this secure technology is available today and at a comparable cost to older, less secure technologies.



## Beware the CSN Pitfall

Another common point of confusion to watch out for is the CSN, or Card Serial Number. Smart cards have not one, but two numbers encoded on the card.

One is the cryptography key that is used to mutually authenticate with the reader. The other is the card serial number—also referred to as the UID or unique identifier. This is a number burned into the card during the manufacturing process.

If you are shopping for an access control system and want to use smart cards, be careful you know and understand the difference between these two numbers.

Eric Widlitz observes that "even today, people buy a smart card and don't really use it as intended for. Every chip has a unique identification number on it. But it is not secured in any way, shape or form on that card. If you are considering purchasing a smart card and only plan to use the serial number, it's no different than using a prox card. This is because there is a single unique identifier on it that's being transmitted openly and in the clear. There's no security behind that."

The smart card's serial number is typically used to identify a type of chip. That serial number was not intended to be used for physical access control and securing one's identity within a security system.

Still, many uninformed buyers end up using the CSN to secure their buildings. "I've seen it not only at schools, but at large enterprises," says Widlitz. "And many times, it's because people don't understand. Or they may have a reader on the wall—it's very simple today to build a reader that will just read everybody's serial numbers."

Sometimes campuses may not have a choice and need to use the CSN if they have multiple buildings with different technologies.

"I would say use that to help you migrate to a secure platform," Widlitz suggests. "But that should never be the intended use of a smart card, to use the serial number as an identifier."

## Your Path to Migration

Like most physical security initiatives, a phased approach is suggested for upgrading your credential technology. To make a migration easier you can use what are called multi-technology, or multi-tech, credentials. These are cards that can include 125 kHz prox, the 13.56 MHz smart chip, and even the magnetic stripe.

The mag stripe is used for your existing dining and financial applications, prox for existing access card readers, and the smart chip for new and future readers you'll install as you migrate away from the prox readers over time.

The readers themselves—or locks with integrated readers—are also available in a multi-technology flavor to accommodate whichever credential you are using.

"Put a multi-technology reader on the wall so anybody new that comes to the facility gets a new smart card. Or if you're slowly going to phase out the older technologies that reader will be able to read the old card and the new card," says Widlitz.

"But that's going to require you to change your entire reader population. If you're not just talking about one site and it's a global organization with sites all over the place, it might be very difficult to do that. A multi-technology card might be easier to help with that type of transition. Or there may be a combination of both—multi-technology cards and multi-technology readers. And the readers are smart enough that you can set them to read one or the other technology in the card depending on what that facility is and the direction you want to go there."

A wise approach as you plan a migration is to figure out which population on your campus needs what technology. This way you don't purchase the most expensive, multi-technology cards for everyone on campus. Those can be reserved for only the students, staff and faculty that require that card technology for the buildings they use.

"That's where you start. Plan the use cases. And then make sure you have a platform that supports those in the short term. And you know the rest of the use cases will come over the next few years."

## How Far Is the Future?

Where is credential technology going next? Will it always stay on the card?

Daniel Bailin, the director of strategic business development and innovation at HID Global, works on figuring out where the industry is heading next. And according to him, the first place everyone is looking to is the smartphone.

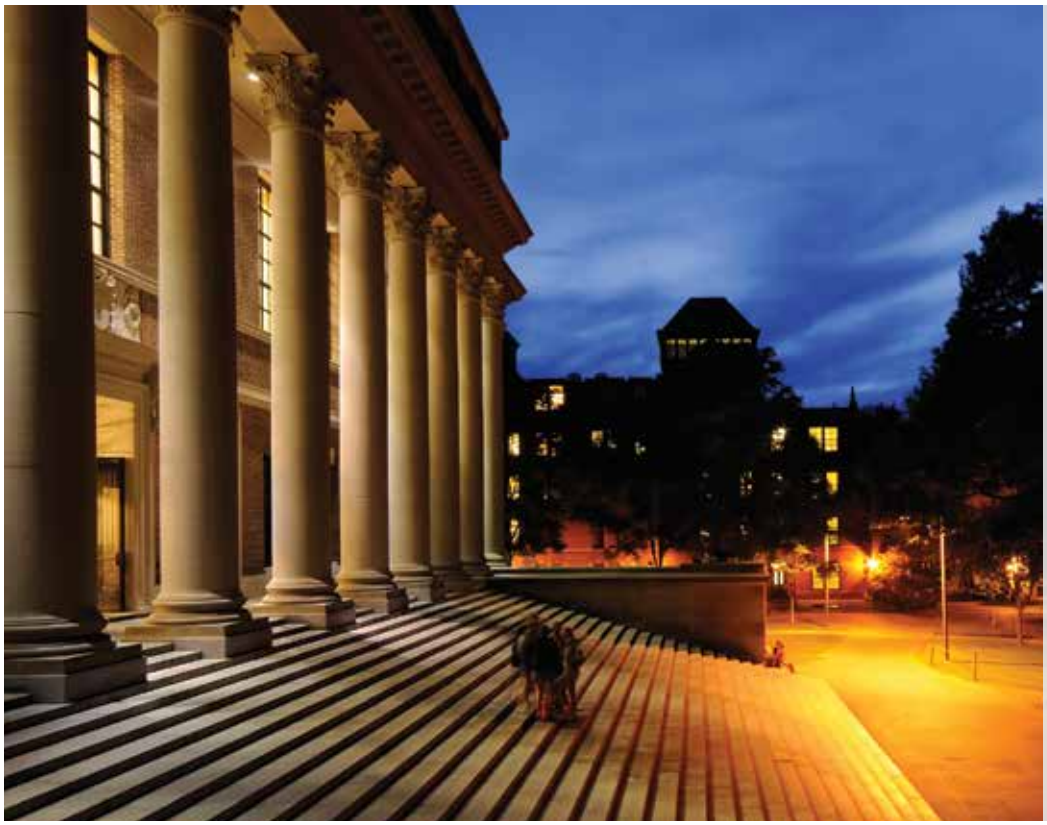
"We're all used to carrying cards to open doors and gain access to other things such as logging into our computers," says Bailin. "It's a natural thing to say now I want to use my phone because I always have my phone with me. Often I have my card, but I always have my phone. And so that's where the focus has been most recently."

But the credential is not stopping with mobile. With people getting used to the idea of using their phones to unlock doors, Bailin and his team look further in the future.

"Now what about wearable technology such as health and fitness devices?" says Bailin, referring to items like FitBits and Apple Watch or Android Wear type devices. "The idea being that if I can use my phone to open the door, why can't I use my wearable device?"

New mobile technologies—like SEOS from HID Global—are being designed to run on any smart device. You can get them on smart cards, phones, and wearables. Even as the payment card industry is moving to the EMV chip, this type of technology can be placed on there as well.

"The idea is to give the people that manage the security in the organization—the IT people and the security people—a choice of platforms they want to support. And ultimately to enable the users to choose the device they want to carry," says Bailin.



*"Don't think you're in the university environment, and three years, five years from now, you're going to tell your students 'you can't use phones.' They're going to expect to do this more and more."*

## Planning Your Roadmap

When starting the conversation about future credentials with security and IT departments, Bailin wouldn't recommend starting with the credential.

"I'd say you would start with finding the solution for the use cases we're trying to harden. We have a use case to open a door into a classroom. We have a use case of getting into a dorm. There's a perimeter secure area, and then there's the actual dorms. So let's now start talking about those use cases."

A trend Bailin and his team are seeing is the convergence of the budgeting process between the physical access side, the security side, and the IT side. And as those come together then they obviously need to plan and budget together.

All parties should set out a plan that in the next few years they should be well on their way towards migrating to a more modern and secure solution.

Something Bailin often sees is people tend to try to solve the problem that's immediately in front of them. For example, a campus might conduct an audit and find a weakness because they use a legacy technology. They know they need to address that. But if they limit the scope to simply solve that immediate problem, they can miss an opportunity to address future issues. Like when are they going to start to support mobile devices?

"Don't think you're in the university environment, and three years, five years from now, you're going to tell your students you can't use phones. I mean, they're going to expect to do this more and more," says Bailin.

As you evaluate the various platforms, think about investing in a platform that has a roadmap to support everything that you might need.

"And even if you don't think you need it today," says Bailin, "it would be naive to think you're not going to have to support these common platforms—phones, wearable devices, in the next, fill in the blank: one year, two years, three years."

The future possibilities of credential technology are exciting, but just like the current options can be difficult to navigate.

"And now it's just up to the IT departments and the security departments to figure out which of those use cases are the ones that we care about," advises Bailin. "That's where you start. Plan the use cases. And then make sure you have a platform that supports those in the short term. And the rest of the use cases you know will come over the next few years."

ASSA ABLOY Americas
110 Sargent Drive
New Haven, CT 06511

ASSA ABLOY is the global leader in door opening solutions, dedicated to satisfying end-user needs for security, safety and convenience

ASSA ABLOY