Debunking the Top 5 Myths about Smart Card Migration for Colleges and Universities

Abstract

Many of today’s colleges and universities are beginning to realize that moving away from traditional magnetic stripe (magstripe) and low-frequency proximity (prox) card technologies in favor of high-frequency, contactless “one-card” technology will provide their students, faculty and staff with a more secure and convenient on-campus experience.

These forward-thinking institutions understand the benefits of utilizing multi-function Smart Cards for accessing a myriad of services and applications campus-wide - from physical facility and logical network access – to cashless payment and tracking time and attendance.

However, although many of these institutions have embraced the idea of multi-function Smart Cards, many still have concerns about the logistics and costs associated with the execution of such a transition. It is precisely these concerns that have kept many universities from implementing Smart Cards even though they realize it is an eventual necessity.

The reality is that many of these concerns, although seemingly valid, are in fact, myths. Such transitions need not be as daunting as perceived at first glance. This Executive Brief aims to take a good hard look at some of these concerns and debunk the top five myths surrounding multi-function Smart Card migration and implementation.

Myth #1: I have to upgrade everything at once – or – I only have one option.

FACT: A phased approach is actually more common and significantly easier to implement for most institutions. If necessary, parallel systems can coexist for months.

Any combination of phased implementation can be executed as needed to meet a specific institution’s needs. Options include:

- Replacing magstripe and prox card readers with multi-technology readers, which will not only continue to support these legacy technologies, but also read more advanced, multi-function Smart Cards.
- Replacing legacy cards with new technology-embedded cards while still preserving magstripe and/or proximity technology.
- Only replace readers and cards for highly sensitive areas requiring additional security, as a first step.
- Begin issuing new multi-technology cards and phase out old ones over time as students graduate.
- Any combination of the above for certain cardholder groups, applications, or buildings.

As institutions research their various options, they should also consider the advantages and potential disadvantages of each approach. For example, although replacing all readers and cards at once may appear to be the most...
streamlined way to project success in terms of shortest time to implement and ability to begin using new applications right away, this approach can be quite disruptive and difficult to manage. It often requires that installations take place at off-peak periods such as summer break. Additionally, institutions find that this “rip and replace” method can be cost-prohibitive.

Replacing a few legacy readers in higher security areas while simultaneously focusing on phased card replacement over time may work best for you. Advantages of this approach often include an overall accelerated transition where institutions can upgrade readers at their own pace, as budget and resources allow and begin to see the benefits of multi-function cards immediately.

For example, if you will be upgrading some readers but only for highly secure areas, you can opt to issue multi-technology credentials only to those who need access to those areas. However, if you will be issuing multi-function cards as part of your “phase I” migration, this will allow for immediate integration of on- and off-campus applications including cashless vending, logical access, or transit and banking services.

Your trusted integrator and vendor such as HID Global can work with you to determine the best approach for your individual needs. Regardless of the upgrade path you choose, you need not be locked into migrating all systems and/or cards at once.

Myth #2: We have too many access control technologies currently in place to migrate smoothly

FACT: Using multi-technology cards, you can migrate smoothly and at your own pace regardless of the various access technologies currently in place.

What many institutions do not realize is that a single Smart Card can securely house up to four different access control technologies including Weigand™, magstripe, low frequency, high frequency or contact chip.

As stated previously, you have the option to upgrade security only for specific departments or facilities/buildings – giving you the option to upgrade readers for only the most sensitive locations now and swap out the rest over time.

The beauty and simplicity of this solution is that multi-technology cards allow students, faculty and staff to enter any location for which they are approved, regardless of whether it has an old or new reader and these combination “high/low” frequency credentials need only be issued to those who need them. Low frequency readers can simply remain in place at standard entrances to less sensitive areas.

So, whether you have multiple access technologies in place left over from past partial migrations or newer technologies implemented to accommodate high-secure areas or even new buildings and facilities, a combination technology card can serve as a very immediate, yet cost effective, first step in your overall upgrade strategy.

Myth #3: It’s not possible to support old and new application technologies at the same time

FACT: Applications that do not support contactless cards – such as library checkout services that still use magstripe or barcode – CAN remain intact and completely operational with multi-technology credentials. Just as multi-technology cards can support various access control technologies, they can also support various applications.
For those institutions wanting to add applications such as that for on-campus cashless vending or off-campus banking and transit, a multi-function Smart Card can be the answer. The card can be encoded not only to support new applications but also legacy technologies that may or may not be part of your overall upgrade planning and implementation strategy.

So, just as with access control, parallel systems and/or technology supporting various types of transaction-based applications can coexist on your campus for months or years as needed.

**Myth #4: Migrations are too expensive to implement**

**FACT:** There is a widespread misconception about the cost of a migration or upgrade. As we’ve already alluded to, your transition can be implemented in phases to align with your investment readiness. What’s more, a large part of existing infrastructure will likely not even require an upgrade, which saves on overall implementation costs. This can include anything from cabling and control panels all the way to individual readers in some cases.

Another often overlooked solution to counter the cost impact of an upgrade is that costs can be shared. For example, when universities identified all of the departments that would be impacted and/or benefit from the upgrade and implementation of multi-application Smart Cards, many were able to unearth additional budget for the project. These institutions found that costs could be spread among multiple department budgets – and a key success factor in securing project budget was obtaining buy-in from various department heads.

Although not the most favorable of topics, when exploring the cost of security upgrades, another recommendation is to consider your risks if you forgo an upgrade. Can you truly afford not to update the security of your buildings or the cards themselves? What would happen if credentials were compromised by counterfeiters and unauthorized parties gained access to the sensitive areas within your campus facilities? How would you recover from a data breach or tragic event that jeopardized the safety of your students and staff and subsequently – the reputation of your institution? These considerations among others should all be taken into account when assessing your potential cost factors.

**Myth #5: Migrating to contactless Smart Cards will slow down the card issuance process**

**FACT:** Encoding need not be a separate step – You can speed the issuance process with inline card personalization. By leveraging ID card printers equipped with internal Smart Card encoders, you can personalize cards both electronically and graphically in a single, seamless step.

Many institutions that issue student ID cards today typically print a card and then encode the card as a separate, additional step in the issuance process. This is generally executed via card services office personnel entering data into an encoder before running the card through to complete the encoding and personalization process. Unfortunately, this approach is fraught with peril as it can take twice as long or more than inline encoding - and significantly increase the chance of encoding errors due to manual data entry inaccuracies.

By leveraging ID card printers that support inline encoding, cardholder data is encoded directly onto the card from its database source, eliminating the “middle man”. Card issuance is expedited and encoding errors are virtually non-existent. Regardless if you plan to use one or more types of encoders...
to accommodate contactless, magstripe or other technologies, more than one encoder can be installed within a single printer to encode cards to your institution’s card requirements.

**Conclusion**

While upgrading to new multi-function smart card technologies are full of exciting and cost-efficient potential, such a transition can seem like a daunting undertaking – especially when working within the confines of a constrained budget or limited IT resources. But today’s institutions need not be distracted by the myths that seemingly stand in the way of upgrading to new technologies that will better serve their constituents. By incorporating a phased implementation approach and leveraging multi-technology cards, successful migration can be achieved in a manner that is in line with your institution’s card program goals and investment readiness.

**About HID Global**

HID Global is the trusted source for innovative products, services, solutions, and know-how related to the creation, management, and use of secure identities for millions of customers around the world. The company’s served markets include physical and logical access control, including strong authentication and credential management; card printing and personalization; visitor management systems; highly secure government and citizen ID; and identification RFID technologies used in animal ID and industry and logistics applications. The company’s primary brands include ActivID®, EasyLobby®, FARGO®, IdenTrust®, LaserCard®, Lumidigm®, Quantum Secure and HID®. Headquartered in Austin, Texas, HID Global has over 2,200 employees worldwide and operates international offices that support more than 100 countries. HID Global® is an ASSA ABLOY Group brand. For more information, visit hidglobal.com