

Migrating from magstripe to contactless access control in higher education

*An examination of the
benefits, challenges
and technology options
available to college
campuses*



Today's colleges and universities are so much more than ivy-covered halls featuring a pipe-puffing professor with leather elbow patches on his tweed jacket. Just as computer-savvy men and women who are anchored in the real world, rather than existing in an ivory tower, have replaced the instructors of yesteryear, so have the security needs for institutions of higher learning evolved.

Universities have an obligation to keep their students safe. Institutions of higher learning must also focus on protecting faculty and other personnel, as well as visitors. Because modern campuses are cities in microcosm, they must meet the additional challenges of protecting the classrooms, housing areas, cafeterias, shopping areas, university offices, stadiums, theaters, libraries, research laboratories, clinics, banks and transportation that are part of today's university facilities.

As an initial effort to secure campuses, colleges began issuing identification cards some 35 years ago. Many of these IDs had magnetic stripes, which were used mostly for the accountability of meals served in dining halls.

Three decades later, multi-purpose ID badges with magnetic stripes for access control, library services and meal tracking are typically issued to students and campus personnel. But magstripe photo ID cards have become inadequate in the face of changing technology, as well as threats to physical and computer security. Violent acts have taken place at many universities, and every campus is potentially vulnerable. College computer systems, which contain a great deal of personal information, must be protected against hacking.

Countless industries, as well as government organizations, have recognized the benefits of moving away from magnetic stripe ID



cards and transitioning to smart cards for increased security. Magstripe technology is both limited and vulnerable to breaches—including counterfeiting. As campus needs have expanded to rival those of modern municipalities, it is imperative that security measures keep pace.

Although some 60 percent of colleges and universities still use magstripe cards as their primary method for access control and payments, many universities have begun to bring their security measures into line with contemporary needs by migrating from magstripe cards to contactless technology. A growing number of schools recognize that the increased security, as well as the convenience, provided by smart cards will enable institutions to be more proactive about protection of students, personnel and physical assets.

Necessary, Practical and Affordable

For many colleges and universities, where the need for increased security is substantial but security budgets are lean, migrating from magstripe to contactless technology may seem out of reach. The reality, however, is that because smart technology is so versatile, the migration can be implemented in stages,

without straining resources.

There are many solid reasons for upgrading to a higher level of access control. No institute of higher learning wants to make tomorrow's headlines because of an adverse incident that takes place on campus. While such an event may not be completely preventable, an immediate response can mitigate the damage. Being able to instantly lock down particular areas of the campus can provide protection for students and faculty during the occurrence and



immediately afterward, while safeguarding the university's reputation.

In addition, some federal mandates require an increased level of security for physical access control to sensitive building space, such as research laboratories, university clinics, and data control rooms. Contactless technology can be used to grant access to certain areas only to authorized individuals. When smart technology is coupled with a compatible computer system, access can be restricted in a matter of moments. By enhancing security to keep people out of places they shouldn't be, such as student dormitories, parents are reassured about safety, which helps position the institution as a modern, desirable place of higher learning.

While a full "rip-and-replace" of all cards and

card readers simultaneously might be an inviting idea, such a measure is usually not feasible from either a practical or a budgetary standpoint. Fortunately, a migration from existing magstripe technology to contactless cards and readers can be completed in stages.

Replacement Timeline

When making the transition from magstripe to contactless technology, the kind of card and the type of card reader must be considered first. Card types include the existing magstripe card, the new contactless card, and a combination card that features both a magnetic stripe as well as a smart-card chip.

The types of card readers include the legacy magnetic stripe reader, a new contactless reader, and a dual reader with the ability to read both the existing magstripe cards and the newer smart cards.

The order in which the old cards and card readers are replaced also must be taken into account when planning the migration to smart technology. If security concerns dictate that all existing students, faculty and college personnel be re-badged immediately, then either smart cards or combination cards can be issued all at once. If contactless, rather than combination, cards are distributed, all card readers will also have to be replaced at the same time so they can work with the new cards.

Alternatively, combination magstripe/contactless cards can be issued first, followed by the replacement of legacy card readers with combination readers. This method is less intrusive and allows for the cost to be spread over several years.

When an immediate transition is not critical, the existing magstripe card readers can be replaced with combination readers. New



buildings, as well as those being remodeled, would also be fitted with combination readers. Contactless cards can then be issued to new students and personnel, or as replacements for lost cards, thus allowing the transition to smart technology to take place over the normally occurring four-year lifecycle of a higher education institution.

Because the Wiegand protocol for security wiring is an industry standard for many different types of readers, contactless card readers can easily be installed to replace magstripe readers without having to make any significant change to the existing wiring or mounting box.

With the options of combination cards and combination card readers, each university is free to replace cards and readers in a manner that makes the most sense, according to its individual security and budgetary needs.

Security, Savings and Convenience

In addition to affording enhanced campus security, contactless technology provides a cost savings in several areas. Maintenance of legacy card readers is an expensive proposition. It is made even pricier because magstripe readers are covered only by limited warranties.

Magstripe technology experiences failures

because it is vulnerable in ways that contactless is not. Magstripe readers work when the magnetic stripe on the card is swiped through the reader, causing the magnetic head to touch the magnetic tape. Various problems can cause magstripe readers to malfunction, including inclement weather. Vandalism can be accomplished as simply as sticking a pencil in and breaking it off inside the reader. Because of these weaknesses, magstripe readers come with only a limited warranty, causing universities to incur additional expenses for repair in cases of malfunction.

Contactless readers, on the other hand, are much more durable. They have no moving parts, so they won't wear out through use. Neither are they vulnerable to vandalism or the environment. But should something go awry with the contactless reader, it is protected against manufacturing defects by a lifetime warranty.

In order for the magstripe system to function properly, not only must the reader be protected, but the integrity of the stripe must also be maintained. Anyone who has experienced the frustration of a hotel room card failure knows how easily a magnetic stripe can become demagnetized or damaged. Magstripe cards don't have to be abused in order to fail: Just the act of swiping the card through a reader contributes to damage of the card surface. And of course, the universities bear the cost when their magnetic stripe cards must be replaced frequently.

The magstripe user also plays a part in the system's functionality. A magstripe card must be removed from the user's wallet and swiped in a certain direction and at a certain speed in order to work.

Smart cards work on RFID technology, which means that they can remain within a wallet or

purse and still work as long as they are close to the card reader. They don't have to be held at a certain angle or waved in any particular direction or at a certain speed. They are not dependent on magnetic coding, so they cannot become demagnetized.

Magnetic stripes also lack intrinsic security and therefore can be easily duplicated. Several universities have been victimized by unscrupulous students who cloned magstripe cards belonging to university officials or other



students and breached the campus security system or generated fake school IDs for profit. These incidents are costly not only in terms of addressing the resulting problems, but also because stakeholders lose faith in the school—not to mention the university's compromised reputation.

Contactless cards feature a chip, and data that is stored on the card is encrypted. For additional security, before encrypted data from the card is transmitted, an electronic "handshake," or challenge-and-response verification, takes place between the card and the reader.

Universities are much less likely to have to replace contactless cards because of failure, and because changes to access can be made easily, students can retain the same card

throughout their college experience.

Smart cards are convenient in many other ways. Aside from using contactless cards for identification and access control, students can maintain just one card for various customized services and payments. Instead of requiring students to carry a library card, meal card, laundry card, PC/printer/photocopier card, building access card and a bus pass, for example, universities can roll these or other functions onto just one smart card. The monetary savings that comes from not issuing and replacing multiple magnetic stripe cards balances out the higher cost of the smart card.

Time and Attendance

Contactless cards can also function as classroom time and attendance cards, should this feature be beneficial to the university. Contactless readers can gather attendance information when students present their smart cards as they enter a classroom. The system can send attendance information to the professor, thus eliminating the time and effort necessary to collect and enter this data by hand. Such a task can be especially onerous in the case of large lecture-hall classes.

When class attendance is calculated as part of a student's grade, contactless technology not only simplifies the process of recording attendance but also provides an electronic trail in case of dispute over whether a student was in class on a particular day.

When staff or students in a particular profession, such as law or medicine, are required to take a certain number of continuing education credits, it is essential that accurate attendance records are kept. Universities employing contactless technology can use it to generate a precise record of participants so that everyone receives the

proper credits and certificates.

Smart cards are also useful to track classroom personnel hours. Teaching assistants and professors who are paid by the class or by the hour can “check in” to their assigned classrooms using their cards so they can be correctly compensated for the time they put in.

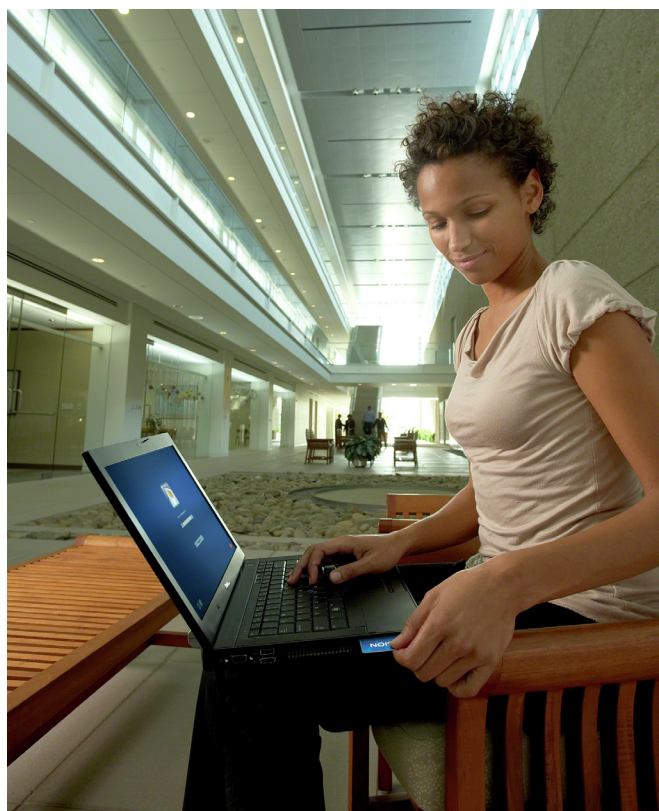
Non-classroom personnel can also use their contactless cards in order to electronically punch in when they access their work areas. The information can be sent to payroll and human resources to ensure that paychecks are correctly calculated. Also, records of punctuality or attendance issues are established. Such data can be analyzed for patterns and any problems that are discovered can be quickly addressed.

Future Trends

Universities must acknowledge their duty to protect students, faculty and personal information—as well as their own reputations. In a world in which campus shootings make the news with frightening regularity and teenagers in their bedrooms can grab personal information by hacking into the networks of major corporations, colleges and universities have to respond by taking appropriate security measures.

Migrating to contactless technology is a painless way to take appropriate, effective and cost-efficient actions. The transition can be accomplished over as short or long a period of time as is appropriate for the individual university. It can be done in stages, and dual-technology cards as well as card readers can be used to ease the migration process.

Once in place, the contactless system can be configured to incorporate additional functions so that it provides much more than



access control. Point-of-sale, transportation, library, printing and photocopying, time-and-attendance, as well as other tasks that haven’t even been invented yet, can be integrated when and as they are needed by the institution.

The contactless card-reading hardware is more reliable than existing readers, and smart cards are more secure, dependable and versatile than legacy cards, offering a highly effective, budget-friendly solution for the modern college or university. ■

Contact: 800.237.7769
insidesales@hidglobal.com

© 2014 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission.