The “check out a book, buy a burger, get in my dorm, catch a bus, take a test, go to the game” Omnipresent Student ID Credential

To Increase revenues, what integrators need to understand about campus cards

April Dalton-Noblitt, Allegion, Director-Vertical Markets

When it comes to big projects and big revenues, colleges and universities can be integrators’ best friends. To help you penetrate this vast market, here is some information which will help you win the project.

In a study conducted among more than 980 American 4-year and 2-year colleges and universities, including leading institutions such as the University of Michigan, MIT, UCLA and Columbia, we discovered what students are using now and what they want to use in the future.

Today, the great majority of colleges still deploy picture ID cards, magnetic stripe cards, mechanical keys and barcodes for access control on campus versus newer, more secure technologies such as proximity and, especially, biometrics and smart cards.

Indeed, 76 percent of colleges still use a magnetic stripe card, even though students are the leading first adapters for new technologies. Only 31 percent of them are using proximity cards, 16 percent are using proximity fobs/tokens, ten percent are using biometrics and nine percent are using smart cards.

What do students want? Convenience is the ultimate student goal. Students want safety and security on campus to be as unobtrusive and transparent as possible. They do not want campus safety measures to interfere in normal activity. Tools that support this goal must enable without intruding. Technology should make their lives more convenient. If technology only “connects” them with the school, they find it not very valuable.

Their One Card systems are perceived as convenient and an enabling connection to accomplish their goals. “My One Card is my everything.” Access to buildings, identification, cafeteria/food courts, library, bookstore purchases, printing and vending, in that order, are the leading applications for which American college students use their school-issued cards.

Although additional features are available, use of One Card systems is inconsistent from student to student and college to college. However, there are three consistent unfulfilled needs that exist for One Card use, students report. First of all, students typically would like their One Cards to replace ATM and drivers licenses to reduce the number of things they need to carry. They want to use their One Card as a debit card and as proof of date-of-birth. Lastly, they want to use it for retailer discounts.

The future credential – students are already carrying it

How about leveraging, as a credential, something students already have? Nearly half of all students identify their cell phones as their favorite personal electronic device. It, too, is their “everything.” Indeed, 91 percent of all mobile users keep their phone within arm’s length day and night. Already, nearly half of all students are using cell phone apps provided by their universities.

Industry Insights

The “check out a book, buy a burger, get in my dorm, catch a bus, take a test, go to the game” Omnipresent Student ID Credential

To Increase revenues, what integrators need to understand about campus cards

April Dalton-Noblitt, Allegion, Director-Vertical Markets

When it comes to big projects and big revenues, colleges and universities can be integrators’ best friends. To help you penetrate this vast market, here is some information which will help you win the project.

In a study conducted among more than 980 American 4-year and 2-year colleges and universities, including leading institutions such as the University of Michigan, MIT, UCLA and Columbia, we discovered what students are using now and what they want to use in the future.

Today, the great majority of colleges still deploy picture ID cards, magnetic stripe cards, mechanical keys and barcodes for access control on campus versus newer, more secure technologies such as proximity and, especially, biometrics and smart cards.

Indeed, 76 percent of colleges still use a magnetic stripe card, even though students are the leading first adapters for new technologies. Only 31 percent of them are using proximity cards, 16 percent are using proximity fobs/tokens, ten percent are using biometrics and nine percent are using smart cards.

What do students want? Convenience is the ultimate student goal. Students want safety and security on campus to be as unobtrusive and transparent as possible. They do not want campus safety measures to interfere in normal activity. Tools that support this goal must enable without intruding. Technology should make their lives more convenient. If technology only “connects” them with the school, they find it not very valuable.

Their One Card systems are perceived as convenient and an enabling connection to accomplish their goals. “My One Card is my everything.” Access to buildings, identification, cafeteria/food courts, library, bookstore purchases, printing and vending, in that order, are the leading applications for which American college students use their school-issued cards.

Although additional features are available, use of One Card systems is inconsistent from student to student and college to college. However, there are three consistent unfulfilled needs that exist for One Card use, students report. First of all, students typically would like their One Cards to replace ATM and drivers licenses to reduce the number of things they need to carry. They want to use their One Card as a debit card and as proof of date-of-birth. Lastly, they want to use it for retailer discounts.

The future credential – students are already carrying it

How about leveraging, as a credential, something students already have? Nearly half of all students identify their cell phones as their favorite personal electronic device. It, too, is their “everything.” Indeed, 91 percent of all mobile users keep their phone within arm’s length day and night. Already, nearly half of all students are using cell phone apps provided by their universities.
And, when it comes to credentials, two-thirds are interested in using their phone in place of an ID card. Why? They feel that they are less likely to lose their phone than an ID card plus they know that ID cards are shared; phones aren’t. Those not interested fall into the students that either don’t have a smartphone or those concerned of a malfunction, such as the battery dying or the Internet dropping.

That day is not that far off as students’ desires for using a smart phone as a credential ties in nicely with the budding discussion of NFC (near field communication) which will inevitably end up on cell phones. No Visa card; no MasterCard card...only their cell phone will be needed for cashless payments or to show their identity.

The smart card, as used in today’s One Card smart card system, would be in the cell phone. For those who worry about batteries running out or the Internet dropping, the smart card technology eliminates such fears. A contactless smart card does not need power or the Internet. As long as the cell phone providers will let the technology work as it can, the two biggest concerns could already be alleviated.

Think about it. We’re already going down the cell phone trail. When you’re not home, home security systems make it easy for you to monitor your home through your web-enabled computer or smart phone. You can check the status of your door locks, grant entry to your home, and turn your lights off and on. And that’s only the beginning.

You can receive text or email notifications when family members access the lock, see what’s happening in and around your house, even when you’re not there. You can conserve energy and save money when you’re away from home by controlling your lights and thermostat.

Reality check on smart phones as a credential

Emerging technology beta sites of such Mobile Keys at Villanova and the University of San Francisco have showcased the possibility of things to come from an access control standpoint. At these universities, mart phones are being used just like contactless smart cards, placed next to the reader to open a locked door. There has been great interest in this future credential by those watching YouTube videos of the demonstrations and interacting with other social media outlets. (http://www.cr80news.com/2012/03/30/villanova-pilot-nfc-video-available-on-youtube)

As earlier stated, the Mobile Keys innovation uses NFC technology within smart phones to emulate smart credentials, allowing use of a mobile phone for entry to secure areas. This functionality relies on phones that are produced with an NFC chip included (or a specific accessory case including this circuitry). With such a phone, the student will simply download an app to create the ability to use the phone as a credential.

The equipment that makes selling the NFC future easier

Besides providing a solution to a type of system that customers will be demanding within the next year or so, integrators need to focus on two things. First of all, the system being selected must be able to read and leverage smart cards. Secondly, you want to set up the infrastructure for NFC now. If you can sell something now that won’t have to be replaced when the customer moves to NFC, you have a competitive advantage.

At Villanova, Schlage AD-Series locks let the university leverage its One Card system to provide safe and secure passage throughout the campus. Administrators can provide seamless integration with their present software, customize today’s access control solution, and easily migrate to future needs when required. Without replacing the lock, or even taking it off the door, administrators can interchange readers and network modules, integrate with existing “One Card” providers via the open architecture platform, leverage their existing network infrastructure, easily upgrade from an offline to a networked solution, change the credentials they are using at any time and use future innovative technologies as they emerge.

There is also an added benefit. The university does not need to tear out its readers when they decide to add NFC throughout the campus. If smart-enabled AD-Series locks or XceedID smart readers are already installed, it’s simply a matter of
downloading the credentials to the students' phones and they are ready to go. If non-smart access technology is being used, multi-technology readers can be installed to help ease into the transition by reading magnetic stripe, proximity and/or smart card ID badges and the smart phones.

That's because all existing 13.56 MHz smart versions of the AD-Series locks and XceedID smart card readers are already compatible with the aptiQmobile NFC technology. No new readers are required.

The future for NFC is imminent

Many smart phones currently on the market are already NFC-enabled with more models being launched every month. In the United States, more than 40 million phones were expected to be NFC-enabled by the end of 2012 and, according to a report by Market Research, nearly half of all mobile phones will be NFC enabled by 2016. Many colleges are very excited about this new technology and its future use.