Identification (ID) cards have become a way of life for students on campuses worldwide. Campuses are turning to smart card IDs as a way to improve security and safety. The cards integrate easily with access control programs and are simple to update with user profile information. They are also easy to deactivate and replace if lost or stolen.

The smart cards contain memory or microprocessor chips that allow them to provide access control, automate certain functions and manage various types of school accounts. The cards provide the user with access to residence halls, libraries, recreation centers and other electronically controlled facilities on campus. They also can act as debit cards for school purchases in bookstores, cafeterias or labs.

While students who carry cards with barcode or magnetic stripe technology swipe the cards through reader devices that retrieve data about the user, contactless smart or proximity cards do not have to make contact with the reading device and transmit data when the user places the card near the device.

As technology has advanced, smart cards now hold more memory and data security capabilities – all at a low cost. For example, when a student drops or adds a class, admissions personnel can use the card to notify the university’s databases. Not only is financial information captured quickly, but the electronic transmission instantly updates the security system. The student can access a new classroom or facility right away, and access to former classroom facilities can be denied.

With a unified approach to access control, campuses are able to enhance their investment in security solutions. Security administrators can create an interface between several systems, including student information, housing administration, and access control, to operate with only one enhanced ID card. Smart cards can be programmed to allow students access to their residence halls, pay for meals at a dining hall, even pay for tickets to campus sporting activities or concerts.
An open architecture credential allows for increased functionality, but on your terms and with the systems of your choice. Other applications can be integrated with the card and additional functionality can be added as the campus grows and needs evolve. A closed or proprietary smart card restricts its use to only the systems that have permission to access the card sectors, thus limiting your choice of available systems.

**Using smart phones like smart cards**

We all rely on our smart phones for more and more every day and students are no different. As Near Field Communications (NFC) technology is now being added to a growing number of mobile handsets, the use of smart phones as IDs on campus is becoming more common and is a convenient alternative to carrying a physical ID card. The smart phone, or mobile ID, can be used for access control, payments around campus, and transit passes just like what is possible with a smart card.

NFC is a convenient way to conduct transactions. NFC provides communication between two devices, such as a phone and access control reader, that are in close proximity to each other, usually by no more than a few inches and has the same enhanced security as using a smart card. It is projected that over 285 million NFC-enabled smart phones were expected to be sold in 2013 and over half the phones sold in 2015 will be NFC-capable.

To turn NFC-enabled smart phones into an access control credential, allowing people to use their smart phones to enter buildings or rooms in the same way they present a badge ID, users simply download the aptiQmobile app to their smart phone. Then, their access control administrator uses the aptiQmobile cloud service to send a secure mobile credential directly to the user’s phone. Once the mobile credential is downloaded, users tap their smart phone to the reader in the same way they use an ID card. Access is quick, easy, and secure.

**Growing uses of biometrics**

Although biometrics first was seen as a high security solution, it now is being used more extensively on college campuses. Biometric systems are more secure than cards or keys because users can be removed easily from the system, and they eliminate the hassle of reissuing credentials.

Another trend will be toward the greater use of biometric profiles, either in a network system or carried with the individual on a "smart card." A hand geometry reader that is integrated with a read/write contactless smart card eliminates the need to distribute biometric templates across a network of readers or to create an access control system to manage the templates. For applications where access points are widespread and difficult or impossible to link in a network, the card makes the use of biometrics easier to implement and manage. In addition, since the template resides only on the card, this solution eases privacy concerns. For systems that are more contained, such as on a single campus, the use of network systems undoubtedly will continue.

**Learn more about smart credentials**

For more information on how to make your credentials work for you, please contact a professional security consultant in your area by calling 888.758.9823 or fill out the Contact Us form on our website at allegion.com.