In the old days, schools relied on people to recognize students entering buildings and classrooms by their looks. As school populations grew and threats to student safety began to rise, identifying who should – or should not – be in a school building has become more difficult. Today’s complex school environments have rendered our old ways of verifying people’s identities insecure and unreliable.

**Card technologies**

Many schools are introducing ID cards to their student populations. These ID cards improve security and students can conveniently use them for cashless vending, check out equipment or resources, charge cafeteria meals and even buy tickets to special events.

There are a number of card technologies available. Cards with bar code or magnetic stripe technology are swiped through reader devices that retrieve limited amounts of data about the user. Contactless smart cards or proximity cards do not have to make contact with the reading device. Proximity cards do not hold any information about the user and are limited in their uses, but are easy to use as they use radio frequency technology to transmit data when the user places the card near a device. To enable the functionality referred to above, it is common to employ smart cards – the most technologically advanced card technology - contain an embedded microchip that carries information about the user. Smart cards allow organizations to store different data in different sectors in the cards memory to enable use of the card with multiple applications within the facility.

Before adding smart cards to your security applications, first assess your needs. By partnering with a security consultant or smart card provider, you can make the task of integrating access and transactions manageable.

Most schools use smart cards to improve the security of their facilities. The card systems add more control over access to school facilities. A card reader located at the main entrance to a building provides a way to monitor who comes into a building. More sophisticated systems can provide real-time links to local law enforcement agencies.
By design, deploying what are called “open” technologies also helps to protect an access control investment for years to come. Smart cards that use open protocols allow school security administrators to focus initially on providing access control to high priority areas, such as classrooms, computer labs and recreation facilities. Other secure areas or applications can be added as the school’s ecosystem expands and security needs evolve because the openness of the card allows it to easily work with many other software and application systems that may be installed throughout a school.

**Electronic access control**
Electronic locks that are used with card credentials have the ability to restrict access to certain individuals, during specific hours or days, or for limited periods of time. Some also incorporate audit trail recording that can be helpful in investigating incidents of theft or vandalism. Card access control systems provide a significant improvement over conventional key-based systems because the cards can be deactivated immediately if they are lost or stolen, and they can be replaced promptly. Cards also can be updated easily by altering a user’s profile to limit or expand access to different areas.

Some electronic locks are designed to protect the investment made for years to come. The modular, scalable characteristics of these systems allow the kind of flexibility needed for growing school districts. As security needs change, the access control software system can be changed, new credential reader modules can be installed, and administrators can choose which openings should remain offline or connected to a network. And all changes can be done without removing the lock from the door.

**Biometric technologies**
Incorporating biometric devices into the system is the only certain way of ensuring that the person being allowed entry is actually the authorized person and is permitted to have access during that time. Nothing else ties a person specifically to a credential.

Hand geometry systems use the size and shape of the hand and fingers to verify identity. Length, width, thickness and surface area of the fingers and hand are measured, analyzed, and the unique features are stored in a template, which is used for subsequent verification.

Fingerprint readers use the unique pattern created by the ridges and valleys of the fingerprint characteristics for identification much as law enforcement agencies have for decades, but they automate the process and integrate fingerprint capture and associated algorithms for template creation into their terminals. Fingerprint recognition works best when applied to smaller populations.

Although biometrics may deliver more security than most educational facilities need, remember that card access systems, PIN codes, keys or other credentials still allow anyone who possesses them to gain entry. They cannot provide total control because they can be lost, stolen, borrowed, copied or otherwise compromised. Also, research shows that people who pose a security threat typically will follow the path of least resistance and choose the easiest targets. By installing an access control system geared to your security needs, you can deter such occurrences up front and reduce the possibility of security breaches, along with associated problems and costs.

**Other security considerations**
If your budget will not accommodate the full access control system you want or need, a system with modular capabilities will make it easier to increase a facility’s level of security when you are ready. If the products available in a proposed system allow it to be upgraded without replacing the existing equipment, cost savings will accrue in hardware, installation, troubleshooting and possibly maintenance.

Wireless locksets work equally well on wood and metal doors, both interior and exterior, as well as glass, monitored and scheduled doors, gates, elevators and portable solutions. Wireless solutions do not need line of sight. Signals
Should students carry a credential?

are able to penetrate cinder block walls, plasterboard walls, brick walls, and many other non-metallic materials for simplified system design and implementation.

No matter how sophisticated your access control system, it is no better than its weakest link. The higher the level of security required for an area or a school, the more important it is to have the strong support of the levels beneath it. All the electronics in the world will not stop an intruder if the lock on a door does not close, latch or lock properly.

Better security can start with a security and safety needs assessment by a qualified security consulting firm. This should be the first step in taking a proactive approach, rather than one that is reactive. This type of assessment, performed by an outside party, focuses on the school’s door openings, key controls, credentials, links with time-and-attendance and personnel scheduling, and other risks inherent with the overall access control system.

Throughout the search for security, it is important to remember that the final choices must comply with local building codes, fire codes and the Americans with Disabilities Act (ADA) guidelines. These factors may add to the complexity but must be considered as part of the solution. A professional security consultant can be a big help in achieving the highest level of security while also ensuring that the facility is code-compliant and ADA-compliant.

Learn more about students and credentials

For more information about smart security that fits into your budget, 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.