

# Access Control

The most recent developments in this area involve the adoption of new identification technologies such as smart cards, biometrics, facial recognition, and integration of access control with other security systems like CCTV and Web-based applications. Smart cards include an embedded chip that can be either a microcontroller with internal memory or a memory-only chip. The card connects to a reader with direct physical contact or with a remote contactless electromagnetic interface.

With an embedded microprocessor, smart cards have the ability to store large amounts of data, carry out their own on-card functions, and interact with a smart card reader. Smart card technology is increasingly being adopted by commercial and government enterprises for ID systems that must support fast, secure, identity verification.

A smart card-based system can deliver a proven, cost-effective solution that accurately verifies cardholder identity. It may also meet the need to protect personal information. Password theft and unprotected PIN-based controls are the top security threats to internal information networks.

Biometric devices have been in use for a number of years, but they have only recently begun to be more readily accepted and implemented due to reliability improvements and price reductions. These technologies measure a wide variety of distinct characteristics, including eye and facial recognition.

The most widely used biometric access controls are hand and finger readers. These technologies are effective not only for access control but also for time clocking and attendance.

Professionals should consider five key issues when examining biometric technologies:

1. **Acceptability.** If people are afraid to use a device, they may not operate it properly. Privacy concerns also must be addressed. The higher the level of security, the more intrusive the biometric. Make sure it will still be acceptable to users.
2. **Ease of use.** People like using security tools that are simple and intuitive. The larger the population, the more critical this factor becomes. For companies many employees, 10 minutes of training time per person can add up quickly-making the enrollment process a nightmare.
3. **Functionality.** How well a biometric system works will determine if it stays on the job. If a biometric feature is working properly, it does two things: allows authorized access and denies trespassers. Biometric devices face two error issues: false accept and false reject. Since every attempt by an authorized user is a chance to make this type of error, this rate becomes more important as the number of transactions increases.
4. **Throughput.** The total time it takes for a person to use the device is a logistical issue that should be considered carefully. This is difficult for manufacturers to specify, since access control is application dependent. Most manufacturers specify the verification time for the reader, but that is only part of the equation. The elapsed time from presentation to identity verification is the verification time. Potential customers must look beyond the verification time, however, and consider the total time it takes a person to use the reader. This includes the time it takes to enter

an ID number, if required, and the time necessary to be in position to be scanned. The total time required for a person to use the reader will vary between biometric devices depending on their ease of use and verification time.

5. Enrollment. The failure-to-enroll rate quantifies how many people simply cannot be enrolled in the biometric device for one reason or another. If too many people cannot be enrolled, the technology simply can't be used.

Facial recognition software is another developing technology. This type of biometrics analyzes facial features and landmark places on the face called nodal points. (There are approximately 80 nodal points on a human face.) Some of the nodal points measured by facial recognition software include: distance between the eyes, width of nose, depth of eye sockets, cheekbones, jaw line, and chin.

In theory, the software program can be set up so only a given percentage of nodal points need to be matched by the computer to yield a positive identification. The software uses an algorithm called local feature analysis (LFA). Each faceprint is stored as an 84-byte file.

Using this methodology, many faces can be stored in a given database using a minimal amount of digital memory. The computer scans the face and then assigns a value using a scale from one to 10. If a score is above a predetermined threshold, the computer declares a match. The operator then reviews the face or group of faces selected from the computer database to determine the correct match.

At present, facial recognition technology holds much promise for ATM security, check cashing identity verification, and elimination of voter fraud because local field conditions can be carefully controlled and monitored. However, reports from the field have claimed that when used to monitor large crowds to locate criminals at large, this technology has not provided optimal results. The problem is that a person must position his/her face a certain distance from the camera in order for a correct identification to be made.

Integrating biometric elements with smart cards and IDs appears to be a rising trend. When a typical badge is lost-from the time it's misplaced to the time it is subsequently reported-that badge is still alive and active in the access control system. By adding a biometric feature to the access control system, a badge alone cannot be used to gain access. Both the badge and the biometric are required, eliminating a possible breach.

Smart cards raise the bar even higher, providing additional capabilities. Facility professionals must be cognizant of the template size required for the integration of smart cards with various biometrics.

While access control technologies are helpful, they are not as important as the implementation of the right system. To articulate the pros and cons of biometric technologies as they apply to individual applications may make the difference in system acceptance by upper management.