Today, an increasing variety of schools, colleges, hospitals and other organizations are looking to technology to address security and safety challenges, including controlling access and improving student and patient safety. K-12 school district officials, for example, seek more effective ways to track student arrivals and departures on school buses in an effort to keep them safe. Universities always need reliable ways to protect high-security buildings, such as research laboratories. Healthcare facilities continuously strive to prevent the spread of infectious diseases by deploying technologies that don’t require a human touch. These are just a few examples.

Standard security protocols such as lock and key, magnetic stripe, and proximity and smart cards have all been deployed to manage building access, but these mechanisms can be lost, shared, misplaced or stolen. With increasing frequency, systems that rely on usernames, passwords and PINs are breached, exposing personal data to fraud that results in billions of dollars in losses each year. Experts agree that campuses require a better way to verify identity.

Now more than ever, security professionals are implementing biometrics into their security protocols because these systems don’t rely on keys or cards, which are easy to compromise. Biometric technology uses a person’s physical as well as physiological attributes, such as his or her iris, fingerprint, DNA, and hand or face, for instance, rather than a card or key to validate the individual’s authorization to access a building, computer network or vehicle.

The advantages of biometrics are significant. With this technology, it is much more difficult to replicate and present fraudulent identity. Users, in essence, cannot forget, lose or have their biometric codes stolen because these “access credentials” are part of their bodies. The deployment of biometric devices can result in significant economic savings for an organization because it reduces the high costs associated with card and key management. Moreover, there are biometric technologies that don’t require the user to make physical contact with a reader or sensor at all, thereby helping to prevent the spread of disease in medical facilities year-round, or at any high-traffic facility during flu season.

One biometric technology in particular that offers statistical advantages that provide value across key security attributes, including speed, reliability, easy-of-use and cost effectiveness, especially in education and healthcare environments, is iris authentication. The iris provides the most distinct qualities...
Blaine Frederick, Global Biometrics Director for STANLEY Security, which offers the EyeLock brand of iris authentication technology, says: “Every day about their children not showing up at home when they’re supposed to,”

Such iris authentication technology at school can greatly reduce this challenge by confirming attendance through monitoring student arrivals and departures via school buses. The technology can also be used to keep track of checked library books, take classroom attendance and support cafeteria point-of-sale.

How can campuses implement iris recognition as part of their security protocols? Once enrolled in the system, faculty, staff and students simply look at the iris reader that is conveniently placed beside or above a doorway, a trestle or even at a computer. The reader then authenticates the individual by taking a simple video of their iris, converting it to a template (code), and then comparing that template to those stored in their database to either permit or deny access to the building, vehicle or network. This technology is also particularly useful for elementary and secondary school districts that must monitor the safety and security of large numbers of children going to and from school on school buses.

“We’ve talked to school districts that field literally dozens of calls from parents every day about their children not showing up at home when they’re supposed to,” says Blaine Frederick, Global Biometrics Director for STANLEY Security, which offers the EyeLock brand of iris authentication technology.

Such iris authentication technology at school can greatly reduce this challenge by confirming attendance through monitoring student arrivals and departures via school buses. The technology can also be used to keep track of checked library books, take classroom attendance and support cafeteria point-of-sale.

Iris Authentication vs. Retina Recognition

There are significant differences between iris authentication and retina recognition. The iris is the colored part of the front of eye, while the retina is the back part of the eye that converts light into signals the brain can understand. Retina scanners shine high-intensity light into the back of the eye through the pupil to capture an image of the vein pattern. Historically, retina scanners have been considered by many to be a highly invasive measure.

By contrast, iris authentication from EyeLock utilizes a simple video camera to identify the enrollee’s iris, much like any person with a smart phone would do when taking a video of a family member or friend. Obtaining this type of data is much easier and less obtrusive than obtaining retina biometric information.
HOW IT WORKS

Iris authentication is second only to DNA in terms of accuracy in authenticating the identity of individuals because of the uniqueness of each person’s iris pattern, as noted earlier. Consider just how unique: no two human irises are alike — ever — not in paternal twins, not in identical twins, not even in the same person. As such, here’s how school administrators, for example, can use EyeLock iris recognition. Students can be enrolled in the system by having video taken of each student’s eyes. This video is then converted into a code (a mathematical representation of the iris). The original image is then automatically destroyed, protecting the enrollee’s identity — and all of this occurs in less than one second. The code is then encrypted for additional security.

Using the school bus example mentioned earlier, once the enrollment process is complete, a student who wants to board the bus can quickly look into a mounted reader without even having to break stride. The system then compares the student’s iris to the template that is stored in the school’s database. If the reader recognizes the student, he or she is allowed access to the vehicle.

How difficult is it to replicate the iris for fooling or defrauding an iris authentication system like EyeLock? The system utilizes liveness and a series of anti-spoofing techniques to ensure that a live person, not a photograph or video, is being authenticated.

“Basically, you can take those 1s and 0s and publish them on the front page of the New York Times, and no one could do anything with them,” says Frederick.

These characteristics remain virtually unchanged from the time of birth. How many are there? In terms of colors, patterns and unique crypts, there are over 240 distinguishing characteristics that simply cannot be replicated. In short, there are no attributes, movements or behaviors of the iris that can be counterfeited.

Beyond schools and universities, iris authentication technology can be utilized across a wide variety of environments and applications. Healthcare campuses, medical centers and doctors’ offices are using iris authentication to verify that patients are receiving the proper treatment and medication, protecting against procedural mix-ups due to mistaken identity. In banking, when integrated into ATMs and bank software architecture, the technology greatly secures transactions to mitigate, if not altogether eliminate, the risk of fraud and identity theft.

IRIS AUTHENTICATION PREVENTS ID THEFT AND SPREAD OF DISEASE

Many in the biometrics field favor iris authentication over other forms of biometrics, including fingerprints and facial scans, because the iris remains biologically constant, making security breaches nearly impossible. Also, unlike latent fingerprints that are left behind and can be copied, the iris cannot be left behind.

Another benefit of iris authentication is that it is an extremely effective, hands-free, touch-free, hygienic technology, preventing the spread of disease. Also, compared to fingerprint and hand geometry readers, which require significant upkeep because users are physically interacting with them, maintenance with iris authentication is a non-issue.

Lastly, some iris authentication technology such as EyeLock can recognize an individual’s iris while at a distance and in motion, at a rate of approximately one person per second. This high throughput...
**Benefits of Iris Authentication**

- Seamlessly combines security and convenience to deliver a trusted, user-friendly means of identity authentication
- Eliminates the hassle and cost of replacing keys, mag stripe cards, proximity cards or smart cards
- Requires less maintenance than other biometric and access control systems, since there is no physical interaction between the users and the readers
- Prevents the spread of germs because it is a hands-free technology
- Allows for high throughput: for example, depending on the make and model, as many as 50 people can be processed through an EyeLock system per minute
- Integrates simply with existing access control and time and attendance systems, for example some EyeLock models connect via Wiegand, F/2/F, Relay and Ethernet

Iris recognition technology can be deployed in a wide variety of environments. Here, an employee is able to quickly enter the office building where he works by looking into an EyeLock iris recognition reader placed on a turnstile.

For all of these security benefits and more, iris authentication is a wise choice for controlling access, not only on school campuses, but in all high-traffic environments where the highest security measures are paramount.

---

**STANLEY. Security**

**High Security. Unmatched Convenience.**

“Ensuring campus personnel can quickly and easily gain access with a blink of the eye while knowing we have the utmost security—that’s my need.”

-Campus Security Director

EyeLock Iris Biometric Solutions, for today’s security needs. STANLEY’s revolutionary EyeLock iris biometric solutions provide fast, accurate, easy-to-use, and cost-effective identity authentication.

1-855-310-1243  |  www.stanleysecurity.com