355 Lexington Ave.
12th Floor
New York, NY 10017
www.eyelock.com

THE EYELOCK DIFFERENCE

08 20 2013

THE EYELOCK DIFFERENCE, IN SHORT

Why should I consider a biometric for Access Control or CyberSecurity in the first place?

The incumbent access control or cybersecurity solutions are based on a card or token, of various types and costs, or user-names, PINs or passwords. The lifetime costs of replacing and managing cards are remarkably high, and the security provided by them is very limited given that cards or tokens can easily be stolen or passed from one person to the next. Moreover, cards are of many formats and types that date back to the 1950s, and so a building with new and old areas sometimes has to support a combination of different formats, which further adds to the cost of card management, and also often requires users to carry multiple cards and to determine which one works for a particular location. This is a very common occurrence in organizations that have grown through acquisition of other groups or companies, or in new buildings where staff from old buildings will also require access so that systems that were designed in isolation now have to work concurrently.

Eyelock's biometric systems in particular do away with that complexity and security risk by replacing the card/token with a person's iris. As such there is no management cost of cards, and no issues regarding legacy or future card formats. It is also highly secure, which not only provides real protection but also makes workers feel more secure in their environment. Most workers know that cards are not particularly secure, and installing a good biometric system is a sign from management that the company values their employees, their environment and the assets with which the employees work.

In Cybersecurity, Eyelock's biometric systems do away with user-names and passwords, which are highly insecure and routinely passed from one person to the next. Moreover, corporate policies requiring frequent changes of passwords often results in workers documenting passwords for easy retrieval by themselves but also fraudsters.

Finally, Eyelock's biometric systems enable the convergence of Access Control with Cybersecurity which in many applications significantly adds value to a security solution. This sounds complicated, but in fact can be as simple as enabling the computer port in a user's room based on their presence in the building as detected by the biometric access control system.

Why should I put Eyelock Biometric devices top of my list for review for Access Control or Cybersecurity?

In short, Eyelock biometric devices are highly scalable, highly accurate, have high-throughput, are easy to use, and are low-cost when integration, maintenance and other lifetime costs are calculated. Other biometric devices score low on many or all of these factors. This is discussed in detail later in this document.

From a user's perspective, Eyelock systems are one of the few access control or cybersecurity technologies that actually increases convenience while at the same time increases security. This is unheard-of in the access control or cybersecurity world, where typically adding security means adding delays or confusion. For example, in an access control pilot for one of our customers, employees refused to allow the device to be moved to a second location since it had become the new gold standard by which they measured convenience of entering the building.

THE EYELOCK DIFFERENCE, IN DETAIL: ACCURACY, EASE OF USE, THROUGHPUT, SCALABILITY, LOW-COST

How is Accuracy measured? Why is Accuracy Important?

Accuracy of a system is typically measured by i) the expected false accept rate (person A is matched as person B), and ii) the expected false reject rate (person A gets rejected as person A). An accurate system needs to have both an excellent false accept rate, and an excellent false reject rate. In applications where a token (e.g. card or PIN number) is used as well as a biometric, then only 1:1 matching is performed. With poorer biometrics like fingerprints, vein and face (see details below) integrators often reduce the match threshold to such a low level in order to minimize false rejects that the value of the biometric in terms of security is limited, even though a demonstration using a few people appears functional.

False Accept Rate

A system with an overall false accept rate of 1 in 100 is not useful in a deployment with 100 workers, and the only viable approach with such a system is to use a token or other means to uniquely identify a person to index into a single biometric for comparison. This has serious negative implications on cost, throughput and ease of use.

On the other hand, a system with a very low false accept rate, as in Eyelock Systems, allows "1 to many" matching, even for millions of users depending on the configuration selected by the integrator. This does away with the token and therefore has very positive consequences on cost, throughput and ease of use.

From a security viewpoint, a very low false accept rate allows a crucial loophole in fraud or criminality of all types to be firmly closed, which is the ability for a user to change or hold multiple identities. Simply checking whether the biometric exists previously at time of enrollment prevents fraudsters or criminals from simply repeating previous bad behavior. This is highly valuable and often overlooked in any security analysis of any access control or cybersecurity application.

False Reject Rate

Biometrics such as fingerprints, vein or face are subject to changes in 3D shape as the user presents their face or their finger or hand, and are also subject to changes in appearance, and artifacts from cuts, dirty fingers, or even atmospheric effects such as dryness. These problems can result in a poor false reject rate, and/or a poor false match rate depending where the integrator has set the threshold. The iris on the other hand is essentially a 2D object neatly tucked away behind the cornea, and is unaffected by such factors. This means that performance is highly repeatable; once a user has learned how to use the system on day 1, then from then on they will get the same performance every day for years.

The iris is also highly stable over time. Small changes over time have been reported in some articles, but this is largely because the iris is so accurate that such small changes can be measured in the first place. It is notable that major organizations such as NIST (National Institute of Standards and Technology) are silent on whether fingerprints change over time or not, largely because so many other factors confound the acquisition of fingerprints, as discussed above.

What is Ease-of-Use? How is Ease-of-Use measured?

Ease-of-Use is a measure of how seamless a device is to use. There is no standard metric for Ease-of-Use, but Eyelock has developed a criteria based on:

i) Waiting time to use the device, particularly for access control applications where multiple people use a single device

ii) Number of discrete steps the user has to perform to use the device,

iii) How disruptive each step is compared to what they would have done if no access control / cybersecurity control point were there,

iv) How similar the steps are from one day to the next.

Why is Ease-of-Use Important?

i) Waiting time is important for several reasons. First, from a productivity viewpoint people are waiting rather than working. Second, our tests have shown that frustration levels and negative focus on the security system rises exponentially as waiting times increase. This can translate into numerous complaint calls per day.

ii) The number of discrete steps that a user has to perform to use the device is important also. For example, in access control applications, the simple process of taking out a card out from a wallet can comprise multiple steps that in isolation can take only 0.5-2 seconds each but in total has a large negative impact on convenience and throughput, for example: i) put down briefcase/bag/coat/coffee to free up hands, ii) Retrieve wallet from pocket, iii) Retrieve card from wallet, iv) Swipe card, v) Put card back in wallet, vi) Put wallet back in pocket, viii) Pick up briefcase/bag/coat/coffee. In many biometric access control systems in use today, only "1 to 1" matching is performed, which means that a card is still required to look up the biometric being used. That means that it is guaranteed that the use of a "1 to 1" biometric system will always negatively impact throughput and convenience compared to a "1 to many" system, since additional steps for the biometric will always need to be added. This is not a particularly compelling prospect for a security manager; deploy a new system and face the prospect of more complaints and negative reactions. This is one reason Eyelock primarily deploys "1 to many" biometric systems for access control applications to eliminate card usage and the associated cost and inconvenience, where it is possible to do so. For cybersecurity the number of steps required is equally important. For example, a common preferred use case is for the user to continually re-authenticate themselves during a laptop session, in some cases every 5-10 minutes. Even adding a simple step such as button presses on a device becomes unacceptable when it has to be done 50 times per day.

iii) The degree of disruption of a step is also important, since more disruptive steps are usually more error-prone and/or take longer, which affects throughput. For example, finding and fiddling with buttons on a device is disruptive since it is error prone (why should I press a button in the first place? which button? when am I done pressing?), and takes time. All Eyelock devices are designed to be intuitive with no buttons to press. Typically with Eyelock devices the user need only take a quick glance at the device and entry is gained if the user is authorized. Our tests have shown that even the process of stopping or starting at the right place and time, even before a biometric is acquired, is hard and confusing for many users to do, and it takes time to do it. That is why almost all Eyelock devices have in-motion biometric read capability that allows an accurate biometric to be read as the person moves, which is a continuation in part of their normal body motion, as opposed to having to freeze at the right place and time in an awkward pose.

iv) The similarity of steps from one day to the next is also important. One of the major problems with fingerprint, face and other similar biometrics is that the performance of the system depends on factors that can vary easily from day to day. For example, the quality of the fingerprint read varies depending on how the user presents their finger precisely, or how hard they press, and can depend on the humidity and also on the fingerprint scan left by the previous user. The performance of face recognition systems can depend on whether you put make up on differently from one day to the next, or shaved, or whether you are smiling or not, or whether the lights in the building have been changed so the person's appearance has changed even minimally. So such a biometric system can work perfectly well for a person one day, but can work perfectly badly the next day. This is problematic not just from a system viewpoint, but also from a user-relations viewpoint, since people tend to remember the time that the system did not work for them, even if it was just once out of 10 times, and complain appropriately. If a system inherently is unpredictable from one day to the next for all users across a usage population, then a security manager should be concerned that he will get at least 1 complaint call from every user in the system eventually, which by most measures is unacceptable. Eyelock systems on the other hand are designed to be

very predictable from one day to the next, over a period of years. This means that if a system works for a user well on one day, then it will work in the same way the next day and so on. This is important since if there are any issues then they are limited to a small fixed number of people that can be managed, typically by re-enrolling or other means, and the likelihood of complaints is minimized enormously. Eyelock achieves this predictability by virtue of its SAMBI acquisition software and hardware design, its BioTag match software, and by use of the iris biometric which is tucked behind the cornea and always has the same shape when presented to the device (unlike a hand, or fingerprint or face, for example).

What is Throughput? How is Throughput measured?

Throughput is the number of people that can go through an access control / cybersecurity point in a given period of time. Typically throughput is measured in people per minute.

Why is Throughput Important?

Throughput is often one of the most overlooked and underspecified requirements, even by the most seasoned integrators or users. In access control applications, tests performed by EyeLock have shown that the highest throughput needs are typically at the beginning of the day, when people typically arrive for work, and to a lesser extent at lunch time. In addition to this, our tests have shown that in urban areas people arrive in waves due to the arrival of a train or other form of mass public transport.

Based on real measurements from our systems, the throughput in the morning period can be as much as 100 times the throughput in an afternoon period.

Throughput capability of a system is critical since, as an example, if people arrive at a rate of 11 people per minute, but a system can only process 10 people per minute, then gradually (11-10) = 1 person per minute is added to a line forming behind the system. After 10 minutes, 10 people will be waiting in line, and after 30 minutes, 30 people will be waiting in line. Each person standing in line is focusing on the access control system for the wrong-reasons. If this happens every day, then the security manager can be sure to receive regular calls from any number of people standing in line. This is why all Eyelock products are designed to reduce throughput. This is not just clever math; a major Fortune

100 company with experienced integrators installed a fingerprint biometric system without full consideration of throughput and invited us to watch the consequences as described above.

In cybersecurity applications, typically only one user uses a device at any one time, but regardless, the throughput or time for that cybersecurity process to occur needs to be as small as possible compared to the process that the cybersecurity process is targeted to protect, in order to be practical and cost-effective. Therefore high instantaneous throughput is also a very significant factor in cybersecurity applications. For example, if it takes 30 seconds to perform a cybersecurity process designed to protect a process that itself takes 2 minutes to perform, then fully 25% of time is spent just authenticating the user. Tests in the banking environment for example have shown that throughput of customers, particularly in bank branches, is directly related to the cost of servicing customers.

What is Scalability?

Scalability is defined in two ways. First, it is the ability to deploy a system so that it can handle 1 to millions of users. Second, it is also the ability to deploy 1 to thousands of access points co-located or distributed internationally, without having to re-design the whole system to suit the new requirements or have to hire biometrics experts to figure out a bespoke solution that will be difficult and expensive for an integrator to maintain.

Why is Scalability Important?

Scalability is crucial since until now, biometrics have been seen as "boutique" technologies only useful in isolated deployments, such as data centers where typically few people work, or as novelty items that remain unused in laptops or cell-phones because of their ineffectiveness as described in this document. In access control applications, deployments have sometimes required custom control boxes to perform biometric matching that in turn require the installation of a control room near the biometric readers. All this adds to cost and disruption, or in some cases is just not feasible. In addition, some systems simply can't handle large numbers of users. For example, some biometric systems can perform matching with a 1 in 100 performance rate, but clearly the addition of more than 100 employees is not then supported. Some systems also arbitrarily limit the number of devices that can be attached to the control box, since they were not designed with scalability in mind.

Eyelock systems on the other hand have been designed to be scalable from the outset. Millions of users can be handled depending on the configuration options used by the integrator. No special local control room or equipment needs to be provisioned. The discussion on the installation of EyeLock systems illustrates the simplicity and scalability of the solution.

As discussed earlier, from a cybersecurity viewpoint, scalability stemming from a very low false accept rate allows a crucial loophole in fraud or criminality of all types to be firmly closed, which is the ability for a user to change or hold multiple identities. Simply checking whether the biometric exists previously at time of enrollment prevents fraudsters or criminals from simply repeating previous bad behavior. This is highly valuable in cybersecurity applications and often overlooked in any security analysis.

In addition, many banking and financial infrastructures have evolved over years by ad-hoc technology initiatives or through company acquisitions that have not had the benefit of consolidation of the technical infrastructures. This is because legacy customers still need to be serviced, but the systems can't be shut down or fail even briefly to accommodate significant changes in system architecture. As a result a customer may be independently indexed on multiple systems in any given banking infrastructure, which vastly increases the cost of servicing that customer since even the most benign customer query can become a forensic investigation to some extent. Eyelock's biometric architecture can span across all these multiple systems, and is an opportunity to link the individual using a unique biometric record that enables simple and low-cost look-up and retrieval of data.

Cost is Important. What is the Total Initial and Ongoing Cost of an Eyelock System compared to others?

For access control solutions, on the face of it a card reader solution can appear cheaper than almost all biometric solutions. However, Eyelock devices have been designed to be very easy to install with no custom control boxes, and with no initial and ongoing card costs. This means that an Eyelock solution can actually be cheaper than a card reader solution if card management and replacement costs are included. Also, Eyelock's focus on simple installation translates directly into cost savings at the initial installation stage, since there is no custom control room to set up, and no custom control boxes to find space for and install.

For cybersecurity, in addition to its standard devices, Eyelock's upcoming miniature Pico device is highly cost effective and overall comparable to token-based devices with none of the drawbacks related to security or inconvenience.

THE EYELOCK DIFFERENCE: QUANTIFIED

Accuracy

Eyelock Systems in standard configurations have a FAR rate of approximately 1 in 1.3 million depending on the integrator configuration and other factors, and can be configured to have an even higher FAR rate using templates from both left and right eyes. Fingerprint, face and other biometric products on the other hand struggle to achieve even 1000 times less accuracy. This essentially precludes other biometrics from being used for "1 to many" applications for transactional, scalable, every-day use.

Ease-of-Use

EyeLock systems typically have just one operational step; glance-and-go. Other biometric systems have many more steps, which can include very disruptive and time-consuming steps such as removing gloves, dropping briefcases, pressing buttons. In addition, EyeLock systems are repeatable from one day to the next; once a user knows how to use the system, then performance is essentially the same for them for years. The performance of other biometrics on the other hand can vary widely from day to day and are subject to environmental conditions (e.g. humidity) or changes in usage (e.g. slightly different presentation of the finger).

Throughput

EyeLock systems have throughput targeted to reach 20 people per minute. Face biometrics can operate at a similar rate, but accuracy and ease-of-use (different performance from day to day) makes their deployment impractical in most applications. Almost all other biometrics have a throughput that is at least 2 to 3 times less. As discussed earlier, even a fractional decrease in throughput (given that all other factors are equal) is the difference between a successful and a failed biometric system. Also note that competitors often only specify throughput in terms of the time their device needs to perform matching. They do not typically account for the gross inefficiencies and negative impact on

throughput resulting from the steps leading up to the biometric match itself, such as putting down a briefcase or taking off a glove.

Scalability

EyeLock systems are designed to work from 1 to many millions of users. Other biometric systems are very limited in scope, and success in such systems is typically declared if a system is deployed with just a few hundred users. In addition, EyeLock systems are designed to bypass custom control boxes or processors, the use of which makes mass installation difficult and expensive.

Cost

On the face of it, for access control solutions a card reader solution can appear cheaper than almost all biometric solutions. However, Eyelock devices have been designed to be very easy to install with no custom control boxes, and with no initial and ongoing card costs. EyeLock can walk you through the cost savings for you particular application.

For cybersecurity, in addition to its standard devices, Eyelock's upcoming miniature Pico device is highly cost effective and overall comparable to token-based devices with none of the drawbacks related to security or inconvenience.

EYELOCK: GETTING INTO DETAILS

How does an Eyelock system work?

In short, a reference iris template is recorded or enrolled for each prospective user. The set of templates is then stored in an iris template database that can reside on an Eyelock device, a user's device or a back-end database. At time of verification, Eyelock devices search through the iris template database in real time. If a match is found, then in access control applications the Wiegand or other standard signal corresponding to that person is sent from the Eyelock device to the access control system. The access control system then sends a signal to open the door or turnstile. Other control options such as direct relay control are also supported.

In cybersecurity applications, encrypted message packets are sent to enable a function, such as disk encryption or remote-login to a web-site.

Are Eyelock devices safe?

Yes. An EyeLock device typically produces less illumination than a small light bulb, and walking out in sunlight for a few seconds exposes the user to many times more illumination than the devices produce. The devices use infra-red illumination, not unlike the illumination used in TV remote controls. More formally, Eyelock devices have passed the stringent CIE Standard S009/E-2002 and ANSI RP-27.1-2005 standards for illumination safety. Eyelock devices in relevant cases have also passed stringent UL 294 and CE standards. These standards not only tests and certifies for safety, it is often a requirement in building regulations for fixed infrastructures due to insurance requirements.

Are Eyelock systems secure?

Yes. Eyelock devices and systems are architected to have a robust, layered security system that addresses security at all points in the system, from the database to the devices themselves.

Is there an Iris Database on the device?

Yes, if wanted, and No, if not wanted. Having an iris database locally means that data does not need to go back to a control room or central database for matching, which can result in slightly increased match speeds. Also if a network goes down, then data is still in the device to allow access. Many other iris systems aren't capable of doing this since they need to be connected to remote processing systems even for basic operation. If a local database is not desired for procedural or other reasons, then a remote database using Eyelock's remote BioTag software can be used. Having a remote database, at least partially, is necessary if a large number of users is expected, as discussed below.

A device holds 5000 users, but I have 100,000 employees? How does this work?

Eyelock devices can actually hold many more than 5000 users on a device, but the time it takes to perform matching on the device when more than 5000 users are in the local database begins to affect throughput. Eyelock's SAMBI and BioTag software allows templates of users to reside both locally and at a remote database, and depending on the integrator's settings matching can be performed at either location. More specifically, templates of frequent users automatically end up residing on the device (configurable from 0 to 5000 users), while templates of other users stay resident at the remote database. The

practical result in access control applications is that special VIPs or other infrequent users are in fact in the database, but it takes slightly longer (+1/2 second typically depending on network speed) to perform matching, while every-day users in the local database get a slightly shorter match response time.

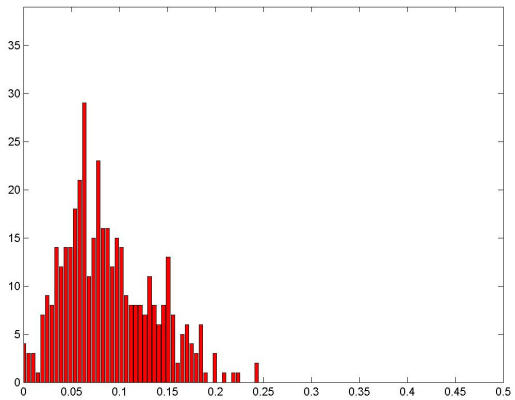
What do FAR and FRR mean?

FAR is the False Accept Rate – the rate at which an incorrect person is matched against a database. FRR is the False Reject Rate – the rate at which data was acquired but was not matched in the database, when it should have.

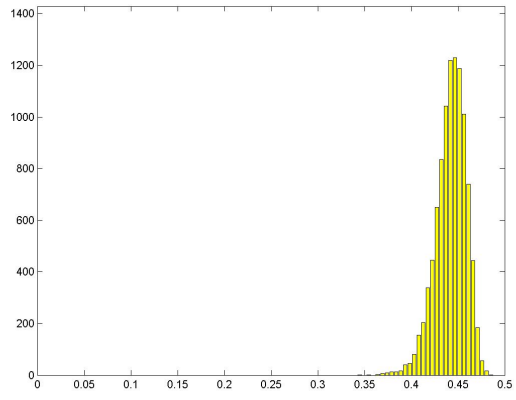
What is FAR, FTA, FRR of Eyelock Systems?

The figures below show the performance of an Eyelock system with 509 users, performing 250 transactions per day on average, with at most 2 retries, over a period of 312 days. Retries are sometimes required to overcome eye-blink or other momentary image acquisition artifacts, and Eyelock devices are designed to make re-tries quick and simple without significant impact on ease-of-use or throughput.

On the left is a histogram of authentic match scores, while on the right is a histogram of impostor match scores. The first point to note is that unlike fingerprint or almost any other biometric systems, the curves are widely separated and do not merge into each other. This means that a single threshold separates the two curves without any performance trade-off. The graph on the right corresponds to 128,286 possible cross comparisons.



Authentic Match Scores



Impostor Match Scores

The graphs show there is 0.0% FAR and 0.0% FRR. Such performance rates are achieved by a combination of Eyelock's SAMBI software that opportunistically acquires the best available eye imagery which other iris systems typically ignore, and Eyelock's BioTag match software that is optimized to work efficiently with SAMBI.

More extensive performance analysis of BioTag has been performed over 3rd party standard iris databases, and this demonstrates similar or even superior performance compared to gold-standard iris match algorithms. More specifically, the impostor distribution of GRI's BioTag is consistently sharper across all datasets with a variance of 2.5e-04, as compared to a standard algorithm, which has a variance of 3.88e-04. This characteristic is responsible for significantly reducing False Accept Rate (FAR).

The mean of impostor curve for BioTag is about 0.445 as compared to 0.458 for the standard algorithm. This is a direct consequence of BioTag's ability to handle larger variation in angular orientation of the eye. BioTag's angular variation has been configured high to handle user tilting his head sideways.

The mean of the authentic curve for BioTag varies between 0.08 – 0.13 for Category 1 and 2 imagery (high and medium quality imagery). This is comparable to the mean of the authentic curve of a standard algorithm, which is 0.110. However, the variance of the authentic curve for BioTag is consistently sharper with a variance < 0.0035 compared to 0.00422. This characteristic is responsible for reduce False Reject Rate (FRR) which in-turn reduce Failure to Acquire (FTA) rates.

It is noteworthy that for poorer quality imagery (Category 3 and 4) of ICE and CASIA databases, the BioTag performance degrades gracefully. The mean and variance of the impostor curve is mostly consistent across all four categories and across all databases. This implies that even as image acquisition quality degrades False Accept Rate (FAR) doesn't increase.

EYELOCK: INSTALLATION

How do I install an Eyelock Access Control system? I already have card readers.

The EyeLock devices are installed, typically 4ft from the floor, using a standard single, electrical recessed mounting box, for example. Power is applied to the device using Ethernet POE+ located in a computer room, or from optional +48V. A small adapter board mounted in the electrical socket or elsewhere connects to the Ethernet wire and sends out Wiegand or other signals. Simply connect the card reader wires to the adapter board instead of the card reader and the device install is complete.

A single new PC computer (or an existing computer) in the control room can be designated to hold the iris template database and the management database software for the devices.

A single new PC computer (or an existing computer) in a guard's station connected to an enrollment EyeLock device by a POE supply and an Ethernet hub can be used for enrollment.

How do I install an Eyelock Access Control system? I haven't designed my Access Control system yet.

The same approach described above can be followed, or an access control system can be chosen that has an SDK that allows direct connection to it over ethernet. This eliminates the need for Wiegand or other control wires, but does require the integrator to write a simple SW interface between the access control system and the Eyelock system, which is straightforward if the access control system uses open communication protocol standards.

How do I manage the transition from a Card-based Access Control system to Eyelock Iris?

In managing a transition, it is helpful to plan assuming that at least a small number of people will still use a card at any moment in time. This may be due to the use of an opt-in policy, for example, where it is unlikely all employees will opt-in overnight. Also, during the transition from card to iris, then a significant number of users may not yet be enrolled or familiar with the system, and a gradual transition over a period of weeks rather than an overnight change is

more manageable by installers and building staff. Typically this can be done by leaving card readers at a few locations as required. Eyelock will also soon offer EyeLock devices with card readers integrated, just for this purpose.

Users can then be enrolled at leisure over a period of weeks or months, preferably before, but can be during or after the installation of an EyeLock system.

Once a particular user is up and running in the iris system then they no longer need their card, and it can be handed in to building security staff.

How do I enroll all my employees?

The first step is to inform users that the biometric system will arrive. A simple email with a link to a simplified FAQ with a diagram provided by Eyelock typically suffices. It is helpful to provide a simple mechanism for users to ask questions. Very few questions are typically asked, but the most common of those questions asked relate to illumination safety, privacy, and in a very few number of cases philosophical concerns relating to technology advancement.

The second step is to enroll users. This can be done before, after or during the installation of Eyelock devices throughout a building. Each enrollment typically takes 1-2 minutes, and there is always a practice test on the enrollment device so that the user becomes familiar with system usage. As discussed earlier, Eyelock devices are highly repeatable, which means that the learning curve for using the device is very small. More specifically, our tests have indicated that after training and the first few uses, performance for subsequent uses are almost identical, which is indicative of the ease of use of the devices.

Obtaining a good enrollment image is key for years of seamless operation for a user, and so time should be spent re-enrolling if necessary.

For access control applications, some of our customers have had "enrollment coffee breaks", where some simple literature (supplied by Eyelock) can be provided, while enrollments get performed. Depending on the size of the organization, multiple enrollment points can be designated, either by moving a single enrollment station from place to place, or by having multiple enrollment stations. All enrollment stations can feed into the same database.

For cybersecurity applications, self-enrollment is possible and Eyelock provides software to enable this if appropriate.

The third step relevant for access control applications is to set expectations to the users on when they will be active in the system. There is a simple synchronization between the iris database and the devices themselves that occurs at regular intervals, defined by the integrator. This is a standard process in any access control system, even card-based systems. Depending on the update rate of the system, it is usually appropriate to tell users that they will be in the system within 24 hours. Setting such expectations prevents unnecessary calls to your staff.

How does the Eyelock Access Control system know the Wiegand or other ID number of my employee?

The simplest way is for the enroller simply to enter in the user ID of the employee at the same time as they enroll the employee's iris. In some deployments an integrator replaces manual entry with a card reader attached to the enrollment PC.

If the Access Control system has a readily available SDK, then this type of integration can happen automatically, but be aware that many access control systems, particularly older systems, have closed architectures that positively discourage such interfaces.

How do I delete a departing employee from the access control database? In general how do I synchronize my access control database to the iris database?

If the access control system has a readily available SDK, then this type of integration can happen automatically, but be aware that many access control systems, particularly older systems, have closed architectures that positively discourage such interfaces. In this case then there are 2 simple methods: first, a guard can simply look up (by name or employee ID) a user in the iris database and inactivate them from the iris system, or second, a report giving employee numbers can be generated by the access control system and the integrator can write simple software that takes the employee numbers and synchronizes them with the Eyelock system.