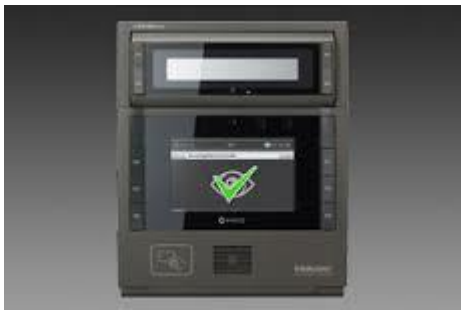
FTL SECURE SOLUTIONS

IRIS RECOGNITION



Iris Recognition is the best of breed authentication process available today. While many mistake it for retinal scanning, iris recognition simply involves taking a picture of the Iris, this picture is solely used for authentication.

What are the advantages of Iris Recognition?

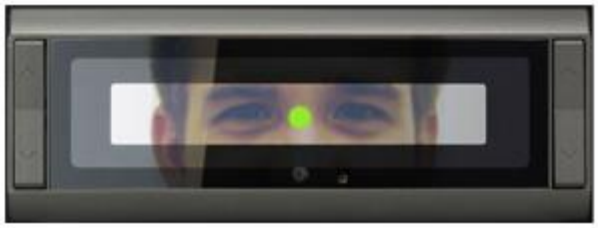
The smallest outlier population of all biometrics. Few People can't use the technology, as most individuals have at least one eye. In a few instances even blind persons have used Iris recognition successfully, as the technology is Iris pattern dependant, not sight dependant.

Iris pattern and structure exhibit long term stability. Structural formation in the human Iris is fixed from about one year in age and remains constant over time. So once an individual is enrolled, re-enrolment requirements are infrequent. With other biometric technologies, changes in voice timbre, weight, hairstyle, finger or hand size, cuts or even the effect of manual labour can trigger the need for re-enrolment.

Unmatched Search Speed. In the one to many search mode is unmatched by another technology, and is limited not by database size, but by hardware selected for server management, in a UK government commission study, Iris ID's Iris Access platform searched records nearly 20 times faster than the next fastest technology, Iris ID has developed a high speed matching engine, Iris Accelerator, designed to deliver 10 million matches per second.

Versatile for the one to many, One to One, Wiegand and Token Environments. While initially designed to work in one-to-many search mode, Iris Recognition works well in 1-1 matching, or verification mode, making the technology ideal for use in multifactor authentication environments where PINS, or tokens like prox or smartcards are used. In a token environment, many privacy issues related to biometric database management are moot, as the user retains control of biometric data – a small template of 512 bytes per iris.

Safety and Security Measures in Place. Iris Recognition involves nothing more than taking a digital picture of the Iris pattern (from video), and recreating an encrypted digital template of that pattern, 512-byte iris templates are encrypted and cannot be re-engineered or reconstituted to produce any sort of visual image. Iris Recognition therefore affords high level defence against identity theft, a rapidly growing crime. The imaging process involves no lasers or bright lights and authentication is essentially non-contact.



Recognition takes just 2 Seconds

Upon approaching a portal detected by Iris Access, proximity sensors activate the ICAM when the subject nears the operational range of the unit. The same mirror-assisted, audio prompted interface that the subject came familiar with at enrolment helps ensure proper positioning and speedy recognition. The ICAM uses the same video and frame-grabbing methodology to create, select and digitise an image to be compared against the stored value retained at enrolment. The live presented value is compared against stored values at the well-secured Identification Control Unit (ICU) assigned to the portal. Once the Iris is matched, either a direct signal is sent to activate a door, or a Wiegand signal sent to a central access panel provides the impetus to open the door to an individual authorised to enter.

How It Compares

Few would argue with the generally held view – and evidence – that iris recognition is the most accurate of the commonly used biometric technologies. There are a number of other factors that weigh heavily in iris recognition's favour for applications requiring large databases and real-time authentication.

Accurate – Like a snowflake, every iris is unique. A subject's left and right iris is as different from each other as they are from any other individuals. It has been calculated that the chance of finding two randomly formed identical irises is on an almost astronomical order of 1 in 10^{78}

Stability – Virtually every other biometric template changes significantly over time, detracting from overall systelabor one does, even weather temperature or ones medical condition can result in template changes in other technologies. Barring trauma and certain ophthalmologic surgery, the pattern in the iris are constant from age 1 to death.

Fast – No other biometric technology is designed to deliver 1-n searching of large databases in real time, A 2001 study conducted by the UK's National Physical Laboratory found iris technology was capable of nearly 20 times more matches per minute than its closest competitor. Looking at speed in conjunction with accuracy, there's simply no other technology that can deliver high accuracy authentication in anything close to the real-time performance of iris recognition.

Non-Invasive – No bright lights or lasers are used in the imaging and iris authentication process. The user can stand as far as 10" away from the unit, and even wear glasses or contact lenses without compromising system accuracy. Unlike some other popular biometrics, iris authentication involves no physical contact, not only does this mean "no touch" authentication, it also means the technology is ideally suited for use in environments where rubber gloves or other protective gear is used.

The Versatility of iris technology lends itself to virtually any application where identity authentication is required to enhance security, ensure service, eliminate fraud or maximise Convenience.