4G Identity Solutions

Authentic People, Unique IDs.

Your Iris is a Unique Key in the World

We are all familiar with security controls that require a card, Personal Identification Number (PIN) or password. These systems are quite common – and all contain an inherent limitation. Each method identifies only the card, code or password, not the person. Cards, words and numbers can be, and often are, given away, sold, stolen – and forgotten. Anyone who can key in a code or flash the right I.D. is assumed to have legitimate access.

The Four Principal Forms of Identification / Authentication:

"What you know" - Password and PIN Numbers

"What you have" - Tokens, Physical keys and Smart Cards

"What you do" - Dynamic Biometrics: Voice, Signature etc.

"What you are" - Static Biometrics: Iris, Fingerprint, Face, Hand Geometry etc.

The most effective method of limiting unauthorized access is biometric technology – identification of an individual by analysis of a physical feature.

What is a Biometric?

Biometric authentication is an automated method whereby an individual's identity is confirmed by examining a unique physiological trait or behavioral characteristic. A behavioral characteristic such as one's signature, voice or keystroke dynamics is influenced by both controllable actions and less controllable physiological factors.

Physiological traits are stable physical characteristics such as Iris Patterns, Finger Print, Face and Palm Prints. Although behavior-based biometrics can be less expensive and less threatening to users physiological traits tend to offer greater accuracy and security. In any case, both techniques provide a significantly higher level of identification than passwords or smart cards alone.

The biometric system first captures a sample of the biometric characteristic during the enrollment process. Unique features are then extracted and converted by the system into mathematical code. The sample is then stored as the biometric template for the enrollee.

The accuracy and performance of biometric based system is measured by the following criteria:
FAR (False Acceptance Rate), FRR (False Rejection Rate), and FER (Failure to Enroll Rate).

Which Biometric?

Points to remember while choosing a Biometric are:

- Proven Highest Accuracy- FAR/FRR/FER
- Speed and maturity of technology-Ability to handle very large Database
- Should remain stable throughout persons life
- Total cost of ownership
- Manufacturer reputation and 'history'
- How critical is the data or physical location being secured
- Convenient hands free operation

	FAR	FRR	FER	Scalability	Interoparability	Encryption	Stability
Iris Recognition	1:1.2 Million	0.1-0.2%	0.5%	1 to all search	Open, Scalable architecure supports interoperable hardware and software	3DES	Very Stable
Fingerprint	vendor specific typically 1:1,00,000	2.0-3.0%	1.0-2.0%	1 to 1 match	Many Vendors, no interoperability standards	Varies with Vendor	Changes
Hand Geometry	vendor specific typically 1:10,000	~ 10%	0.0%	1 to 1 match	Several Vendors, no interoperability standards	Varies with Vendor	Changes
Facial Recognition	vendor specific typically 1:100	10-20%	0.0%	1 to 1 match	Several Vendors, no interoperability standards	Varies with Vendor	Changes

* For complete Report Please Refer - Biometric Product Testing Final Report (19 March 2001, Center for Mathematics and Scientific Computing, National Physical Laboratory, UK).

Iris Recognition

A Unique Biometric Technology

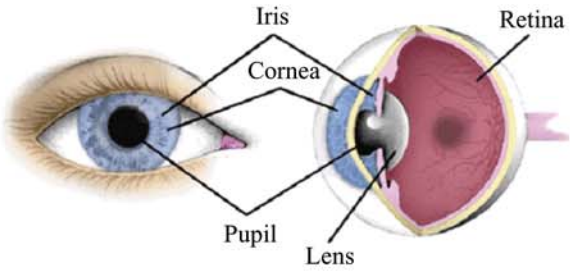
4G Identity Solutions
Authentic People, Unique IDs.

What is the Iris?

Iris recognition is the most powerful biometric technology. There is nothing else comes close.

The iris is the plainly visible, colored ring that surrounds the pupil. It is a muscular structure that controls the amount of light entering the eye, with intricate details that can be measured, such as striations, pits, and furrows. The iris is not to be confused with the retina, which lines the inside of the back of the eye.

No two irises are alike. There is no detailed correlation between the iris patterns of even identical twins, or the right and left eye of an individual. The amount of information that can be measured in a single iris is much greater than fingerprints, and the accuracy is greater than DNA.



Your Iris is a Unique Key in the World

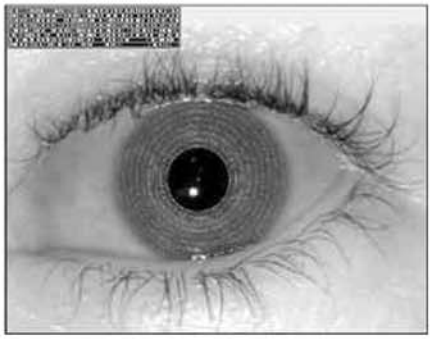
How Iris Recognition Technology Works

Taking a Picture

An iris recognition camera takes a black and white picture from 10 to 24 inches away, depending on the type of camera. The camera uses non-invasive, near-infrared illumination (similar to a TV remote control) that is barely visible and very safe. Proof Positive certified cameras are in compliance with all applicable international illumination safety standards, including ANSI/IESNA RP-27.1-96 and IEC 60825-1 Amend.2, Class 1 LED. These are the latest worldwide standards.

Unlike other biometric technologies that can be used in surveillance mode, iris recognition is an opt-in technology. In order to use the technology you must first glance at a camera. Iris recognition cannot take place without your permission.

Creating IrisCode®



The picture of an eye is first processed by software that localizes the inner and outer boundaries of the iris, and the eyelid contours, in order to extract just the iris portion. Eyelashes and reflections that may cover parts of the iris are detected and discounted.

Sophisticated mathematical software then encodes the iris pattern by a process called Demodulation. This creates a phase code for the texture sequence in the iris, similar to a DNA sequence code. The Demodulation process uses functions called 2-D wavelets that make a very compact yet complete description of the iris pattern, regardless of its size and pupil dilation, in just 512 bytes.

The phase sequence is called an IrisCode® template, and it captures the unique features of an iris in a robust way that allows easy and very rapid comparisons against large databases of other templates. The IrisCode template is immediately encrypted to eliminate the possibility of identity theft and to maximize security.

Iris Recognition

In less than a few seconds, even on a database of millions of records, the IrisCode® template generated from a live image is compared to previously enrolled ones to see if it matches any of them. The decision threshold is automatically adjusted for the size of the search database to ensure that no false matches occur even when huge numbers of IrisCode templates are being compared with the live one.

Some of the bits in an IrisCode template signify if some data is corrupted (for example by reflections, or contact lens boundaries), so that it does not influence the process, and only valid data is compared. Decision thresholds take account of the amount of visible iris data, and the matching operation compensates for any tilt of the iris.

A key advantage of iris recognition is its ability to perform identification using a one-to-all search of a database, with no limitation on the number of IrisCode records and no requirement for a user first to claim an identity, for example with a card.

To discuss how we can help your organization, Please contact sales@4Gid.com

4G Identity Solutions Private Limited, 241, Prashasan Nagar, Road No. 72, Jubilee Hills, Hyderabad - 500 034, India, Tel: +91-40-23558789, Fax:+91-40-23558769

www.4Gid.com sales@4Gid.com