Security solutions
as individual as you are.

CAPTURING YOUR DATA

When registering a fingerprint an **ievo** reader will scan and extract data using an extraction algorithm which identifies specific features within a fingerprint called minutiae.

Identified minutiae points are categorised into groups, which include line bifurcations and ridge endings amongst other data groups. During the acquisition process, the algorithm will identify the type, direction and distance between minutiae which is calculated to create a '2D digital wire frame'. This extracted data is transferred and stored in a database on an **ievo** control board as a template (using AES 128bit encryption). The original fingerprint image is not stored or recorded (See Fig.1).

When using a reader for access a similar process described above will commence. However, this time an additional matching algorithm will be used to compare the new minutiae data against the stored templates in the database. Once a pre-set number of minutiae points have been matched against a stored template, the user's identity will be confirmed, this confirmation will be forwarded to the access control system or 'time and attendance' system for entry and/or data logging.

YOUR DATA

An advanced binary encryption algorithm is used to encrypt specific fingerprint data captured during a scan. This data is used to create a '2D digital wire frame' which is transferred to the **ievo** control board where it will be stored as a user, or fingerprint template. All other information is not stored or recorded. The data CANNOT be used to re-construct a fingerprint image.

SECURITY

ievo systems function with a separate control board which controls an **ievo** reader, meaning that no information or data is stored locally on reader units themselves. For additional security, data captured by the sensor is stored on the **ievo** control board, which will be installed on the secure side of an entry point away from the reader units.

ievo readers also do not house any locking mechanisms or door relays, meaning that if a reader was removed, your access point would remain secure and your data would remain safe. The reader unit would be deemed useless to the attacker, as it contains no data.

DATA PROTECTED

Once a fingerprint has been scanned the original image is not stored or recorded. The only recorded details are the data points taken from a fingerprint which are encrypted and stored on an **ievo** control board. The encrypted data (the '2D digital wire frame) is stored as a user, or fingerprint template and is only accessed for identification purposes within the **ievo** control board. The data cannot be accessed for any other purpose nor can it be viewed using common software. The binary code created by the algorithm is extensive in size and cannot be reverse engineered to recreate an image of the original fingerprint.

To find out more information about **ievo** fingerprint readers and data protection, please contact us.

Fig .1

Image depicting what an **ievo** reader scans.

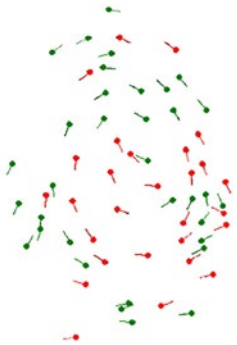

Image depicting data which is encrypted as a '2D digital wire frame'.

To find out more, visit:
www.ievoreader.com

email us at:
info@ievoreader.com

or call us on:
0845 643 6632 or
+44 (0)191 296 3623