



Security solutions
as individual as you are.

Data Protection



How biometric fingerprinting protects you...

Biometrics is the technology of measuring and analysing biological data. For security purposes this biological data can be used to protect you and the premises upon which they are installed. Because of this, your data is used in a certain way which means you must be informed of data protection and how your data will be used.

INTRODUCTION

Biometric fingerprinting is a form of security and has many advantages. **ievo**® in particular aims to protect not only the building or premises being secured, but the users also. However, you need to be informed by your site administrator why your data is being taken, how it is being used and stored. As expected, many of you have questions surrounding the technology, regarding data protection and security. The purpose of this information sheet is to supply you with answers to these questions.

SECURITY

When you have your fingerprint(s) registered on the **ievo**® system please note that the actual image of your print is not stored. Yes, the fingerprint sensor will scan your print upon registration and produce an image initially, but this is quickly transformed into a fingerprint template.

Figure 1 shows an image of a fingerprint which has many reference points, different shapes and unique patterns. **ievo**® scans your print and looks for up to 100 data points, selecting the most prominent identification patterns. This image is converted into binary coding, which is then encrypted via a mathematical algorithm into a **fingerprint template**.

Therefore, the **ievo**® unit itself does not store any visual images. When a user scans a fingerprint the process is performed as previously described. As long as the algorithms final calculation matches a stored and authorised code on the database, then the user is granted entry.

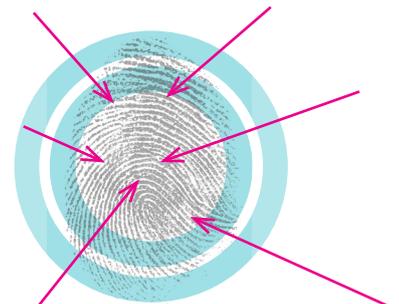
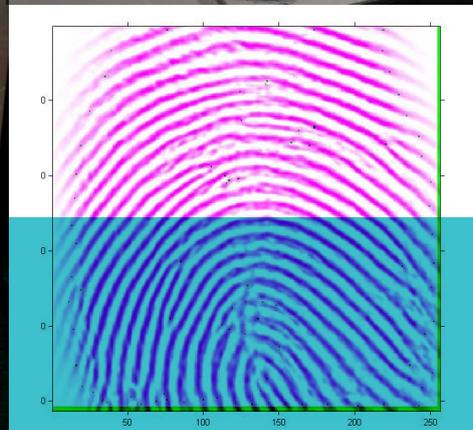


Figure1.



Security solutions
as individual as you are.



UNDERSTANDING TEMPLATES

Perhaps you are wondering where this fingerprint template (numerical pattern) is stored. Many competitive biometric systems store this information in the actual product itself, **ievo**[®] doesn't! Although the fingerprint pattern is unusable outside the **ievo**[®] system, **ievo**[®] have gone further than this by taking extra security precautions and storing the fingerprint templates on the control board which is installed up to 5 metres away on the opposite side of the secured door. Therefore, it is fully protected! It is also worth noting that if someone was to remove the **ievo**[®] unit from the secured door, the entrance would remain closed and the product deemed useless to them.

DATA PROTECTED

First and foremost because of the process described on the previous page, the set of numerical codes and patterns that are created from your fingerprint image are useless outside of granting you access to the secured area. In this way, the pattern is unusable to Police, potential hackers or thieves.

For example, if someone took the fingerprint pattern that **ievo**[®] created for you to a Police Station, and tried to run it through a criminal database, it wouldn't work. The reason being, the numerical pattern that the **ievo**[®] system created for you is unique and protects the image of your fingerprint.

If you would like more information on this, please refer to the **ievo** end user guide.

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

email us at:
info@ievoreader.com

or give us a call on:
0845 643 6632

