  

What is a biometric algorithm?

When the thumb is scanned, an individual templates is created which is then encrypted using a 256 bit AES key that is built into the scanners hardware. The file is then further encrypted using a different 256 bit AES key built into the matching algorithm supplied by Secugen and generated by a unique license purchased for each site. This is more secure than the ANSII and ISO standards that government department’s use as the Secugen Template is encrypted and the ANSII and ISO standards are not.

**The template data is useless and cannot be interpreted back into a usable fingerprint image.** If this was not the case then there would be no world standards and performance measures for such technologies. The data is stored in an array in the RAM of the Biometric Controller and is also permanently stored on the hard drive of the Bio Controller to be restored in the event of a reboot.

*Below is an example of a template code for an individual finger:*

0X417741414142514141414445415141414151415341414D415A4141414141414174774541414C714777346C5869656D6C574945494A764A6B42466D6837616C4E764D704F517874517A706A4A395A31784935686C4177395366726E777645576357386C4573314B426F47443166694170675559704C763168423642682A7043

Please note:

* The solution is secure because the matching can only be done by the individual’s consent as the finger has to be presented to the device for matching. **JRCS and NRS do not hold images of fingerprints in any system**;
* The technology provided for this method of identification meets with ICT Services for Education guidelines;
* Under the data protection act JRCS and Aspens catering cannot allow access to this data by anyone for any other means than for the purpose the data was collected and that is to identify an individual at the till in the catering areas of the school;
* Any biometric data that belongs to an individual that leaves the school is purged which also is in line with the ICT Services for Education guidelines.