timeware®
workforce management solutions
COMMUNITY

timeware® Professional biometrics

Document t2-0451: revision 2.0

www.timeware.org
+44 (0)1706 659368

For more information about timeware® products, version updates, datasheets and reports, please refer to the timeware® community website:

www.timeware.org

NMD³ Ltd

Contents:

What are biometrics?

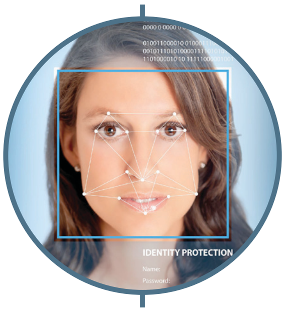
Biometrics is the science and technology of measuring and statistically analysing biological data. In the time management industry, biometrics usually refers to technologies for measuring and analysing human body characteristics such as eye retinas and irises, facial patterns, fingerprints, and hand measurements.

Eyes - Iris & Retina Recognition

The use of the features found in the iris to identify an individual.

The use of patterns of veins in the back of the eye to accomplish recognition.

Face Recognition



The analysis of facial features or patterns for the authentication or recognition of an individual's identity.

Fingerprint Recognition

The use of the ridges and valleys (minutiae) found on the surface tips of a human finger to identify an individual.

Hand Geometry Recognition

The use of the geometric features of the hand such as the lengths of fingers and the width of the hand to identify an individual.

Which biometric technology is the ideal solution for your requirement?

Biometrics eliminate 'buddy punching". No more falsified time cards. No more unauthorised access to restricted area of your buildings.

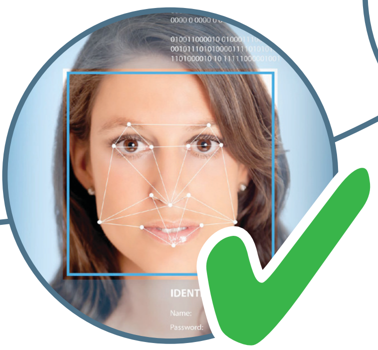
Biometric solutions are better suited for attendance, access and job costing than mag-stripe badges and proximity cards because a biometric data cannot be replicated.

Consequently, there is no on-going cost with biometrics. No-more ordering replacement cards and remember, a fingerprint reader requires virtually no maintenance – an occasional wipe with a soft cloth will clean a reader fitted in the most dirtiest environment.

Fingerprint biometric systems are extremely accurate, quick to implement, and cost effective.

Readers too large for access control. Can be light sensitive.

IP67 - Waterproof. Perfect for internal / external attendance, access control and job costing installations.



Non IP rated. Perfect for internal attendance and access control installations.

Expensive. Not suitable for multi-door access

Thinking of introducing biometrics into your company?

Introducing a biometric system often causes employees to raise the issue of 'lack of trust in the workforce'. timeware® strongly recommends focusing on positives such as accurate data collection which in turn provides an error-free payroll, more reliable fire roll-call reports and when access control is being considered, improved security for the workforce.

THE LAW ON BIOMETRICS
Several pieces of legislation are relevant to the issue of biometrics, but of these the Data Protection Act 1998 is the most important. The Act provides a framework to ensure that personal information is handled properly and provides individuals with rights, such as the right to find out what personal information is held on them.

The Act stipulates that anyone processing personal information must comply with eight principles. They are:

1. **Fair and lawful processing of data**
2. **Processing for limited purposes**
3. Adequate, relevant and non-excessive storage of data
4. Keeping data accurate and up to date
5. **Ensuring data is not kept for longer than is necessary**
6. Ensuring data is processed in line with other rights
7. **Keeping data secure**
8. Ensuring data is not transferred to other countries without adequate protection

Device:	Suprema BioLite N2
Use:	Attendance / Access / Assembly
Rating:	IP67
Location:	Offices, wash-down areas, open-air workshops, external walls
Prox:	Various

The first, second, fifth and seventh principles (highlighted) are the most relevant to this issue. The protections they provide are as follows:

1. Fair and lawful processing of data requires that employers ensure that staff are informed about and understand the purpose for which their personal data is being processed. timeware® uses this data to

a. ensure that timekeeping & data collection records are accurate.

b. ensures a secure environment offering a high level of physical access control.

2. Holding biometric data for limited purposes means that it should not be used for any purpose not directly related to that for which it was collected.

timeware® biometric data is not only held as template data but is also encrypted within the SQL database.

5. Ensuring personal data is not kept for longer than it is needed. This means that biometric data on staff should be destroyed as soon as they cease to be employed by that employer.

On timeware® biometric installations, a special script ensures that an employee's biometric data is automatically destroyed 30 days after they are flagged as leaving the employment of the company.

7. The security principle means that biometric data should be protected against unauthorised processing and accidental loss, destruction or damage.

timeware® ensures that biometric data is encrypted but it is the companies responsibility to ensure that system backups are kept up-to-date and that system passwords are never compromised.

There is nothing in law to stop employers introducing biometric monitoring in the workplace if they satisfy the conditions set out above.

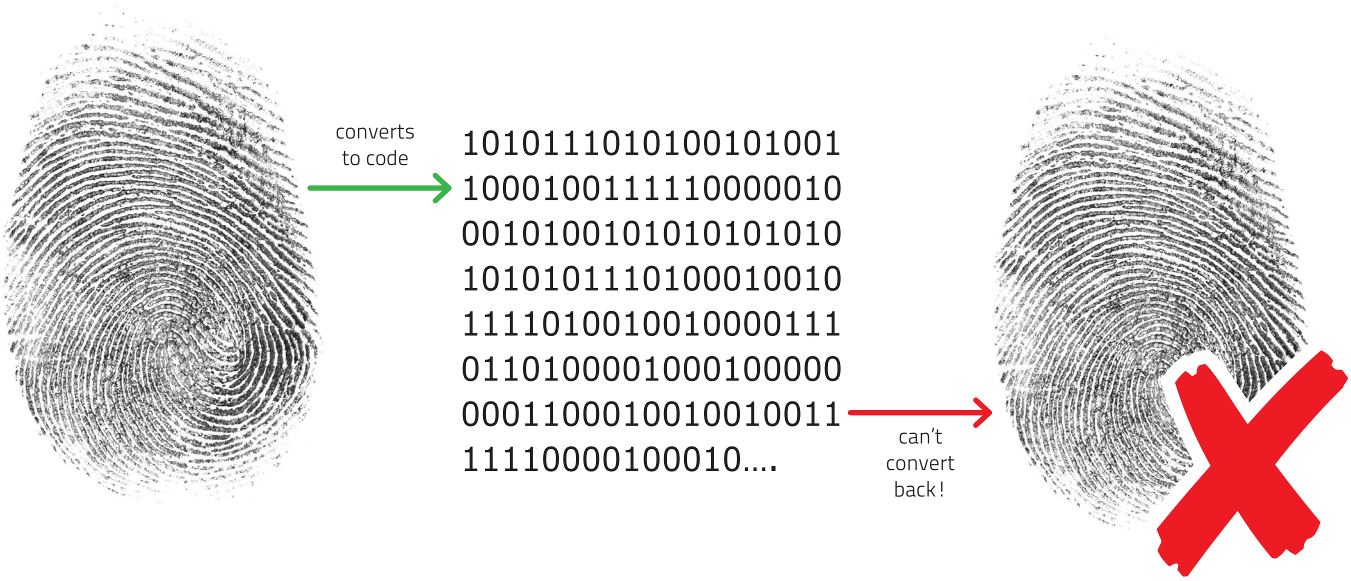
Device:	Suprema FaceStation 2
Use:	Attendance / Internal access
Rating:	No IP rating
Location:	Offices
Prox:	Various

timeware®
workforce management solutions
COMMUNITY

Can an employees fingerprint or facial image be recreated? No!

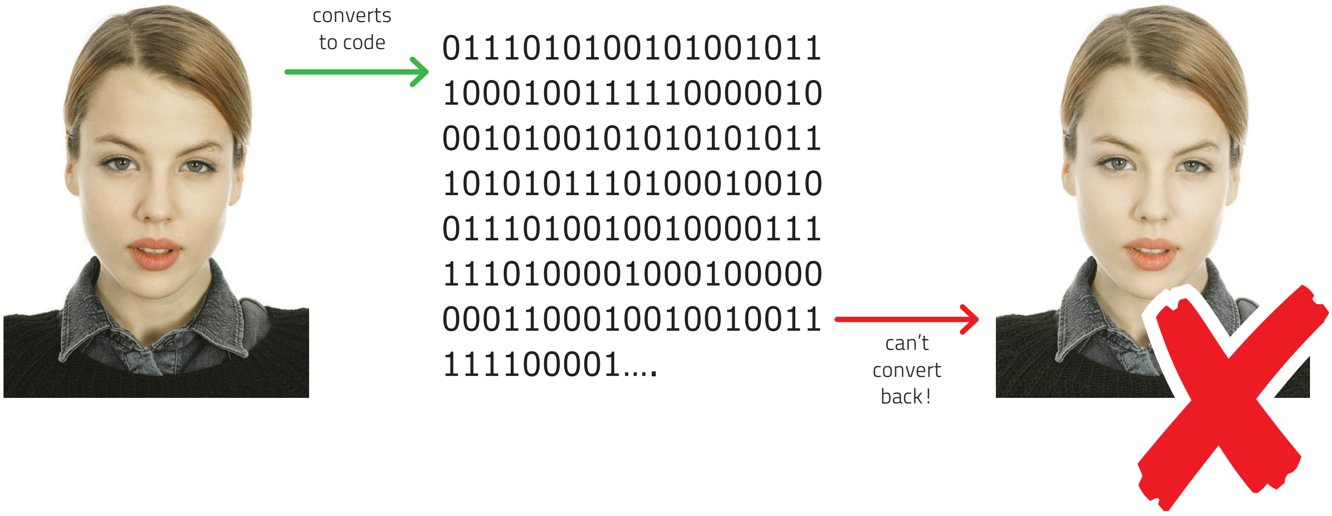
timeware® biometric devices never store an image of your fingerprint or face.

The fingerprint sensor identifies unique minutiae points and measurements within your fingerprint and creates a digital template (not an image) for matching.



```
1010111010100101001
1000100111110000010
0010100101010101010
1010101110100010010
1111010010010000111
0110100001000100000
0001100010010010011
11110000100010....
```

The face sensor identifies unique points and measurements within your facial image and creates a digital template (not an image) for matching.



```
0111010100101001011
1000100111110000010
0010100101010101011
1010101110100010010
0111010010010000111
1110100001000100000
0001100010010010011
111100001....
```

So what is a template?

A template is a set of lines, angles and measurements (minutiae) based upon the unique characteristics of an individual's fingerprint or facial image. These details are captured upon enrolling a person's biometric data into the system, and later used for 1:1 or 1:n matching.

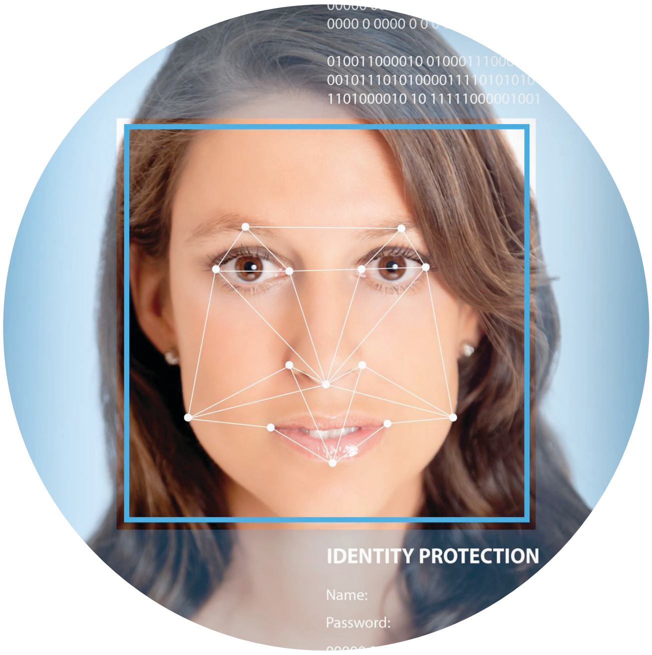
No images are stored in the timeware® database - the template is simply a mathematical representation of your biometric data's unique characteristics.

When recording fingerprints, two templates per employee are stored. The templates are referred to as the primary and secondary templates.

When recording facial data, many images of the face are captured and stored as a single template.

It is important to note that timeware® biometric templates are encrypted and cannot be reverse-engineered to recreate the original image.

timeware® uses Suprema biometric technology which is widely recognised as a world leader in its class.



Now for some technical stuff: "What is 1:1 and 1:n matching?"

1:1 matching is the name for verification

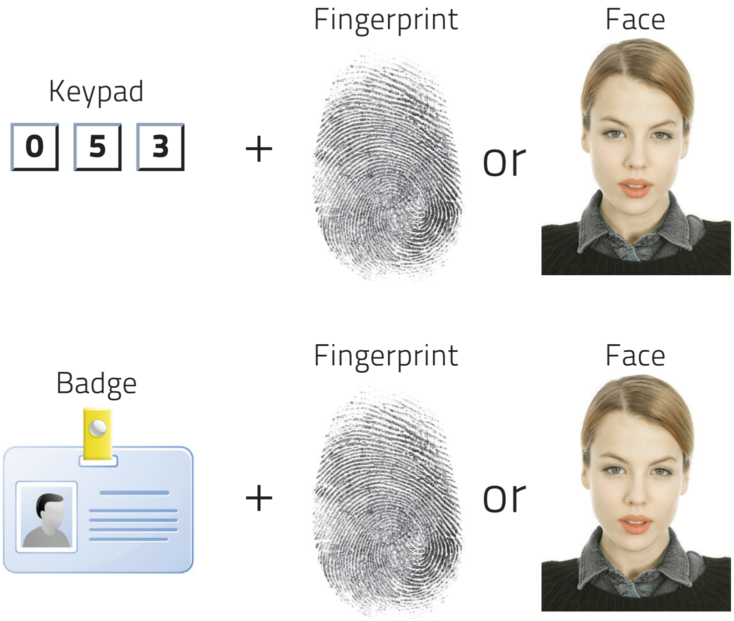
This is a method of examining one biometric record against another in order to determine whether the two match.

This is the type of biometric match that occurs when a biometric system is set up for badge plus finger matching.

The user presents a badge or enters a number which tells the biometric reader who the user is supposed to be.

The user then proves their identity by scanning a finger on the device.

This type of matching is very fast and accurate, and has been in use for some time.



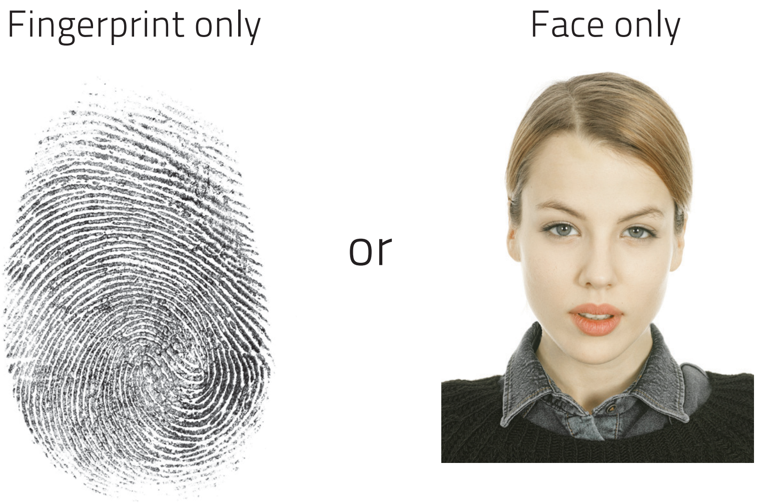
1:n matching is the name for identification

1:n matching is a means of identifying a person against a broad database of other users simply by means of a fingerprint.

The user simply places his / her finger on the biometric reader, and a very rapid search is initiated in order to find and verify the user's identity.

This type of matching is more convenient since no PIN numbers or cards are required.

This is the most popular method and is used by the majority of timeware® biometric installations



Why are timeware® biometrics better than others?

timeware® have standardised on Suprema biometric technology which is widely recognised as a world leader in its class.

Device:	timeware® v13
Use:	Attendance / Job Costing / Cost Centre recording
Rating:	No IP rating
Location:	Offices, Canteen Area
Special features:	ESS, SmartBooking®, Fully Customisable.
Prox:	Various

Device:	Suprema BioLite N2
Use:	Attendance / Access / Assembly
Rating:	IP67
Location:	Offices, wash-down areas, open-air workshops, external walls
Prox:	Various

Device:	Suprema BioEntry P2
Use:	Access / Assembly
Rating:	No IP rating
Location:	Offices, reception, cafeterias, dry workshops
Prox:	Various

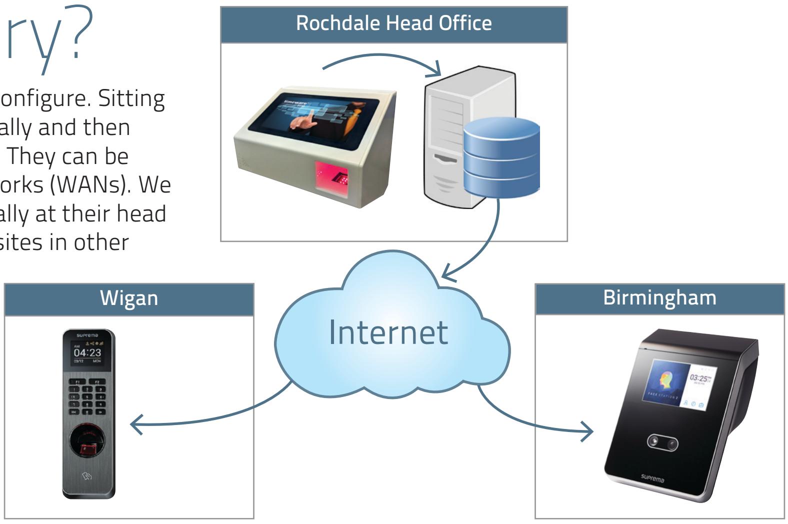
Device:	Suprema BioEntry W2
Use:	Access / Assembly
Rating:	IP67/RK09
Location:	Offices, wash-down areas, open-air workshops, external walls, public areas
Prox:	Various

Device:	Suprema FaceStation 2
Use:	Attendance / Internal access
Rating:	No IP rating
Location:	Offices
Prox:	Various

Can timeware® biometric devices be installed at different locations around the country?

timeware® biometric devices are simple to install and configure. Sitting on your standard network, they collect information locally and then pass the data back to the software every few seconds. They can be installed on both local networks (LANs) and wide networks (WANs). We have many customers that have devices installed initially at their head office and then expanded their system to incorporate sites in other towns and even other countries!

Here is a simple diagram of a multi biometric device installation with the head-office in Rochdale and two remote sites, one in Birmingham and one in Wigan. Please note that if one of the sites closed down, say Birmingham, the device could be very easily relocated to a new location anywhere else in the country.

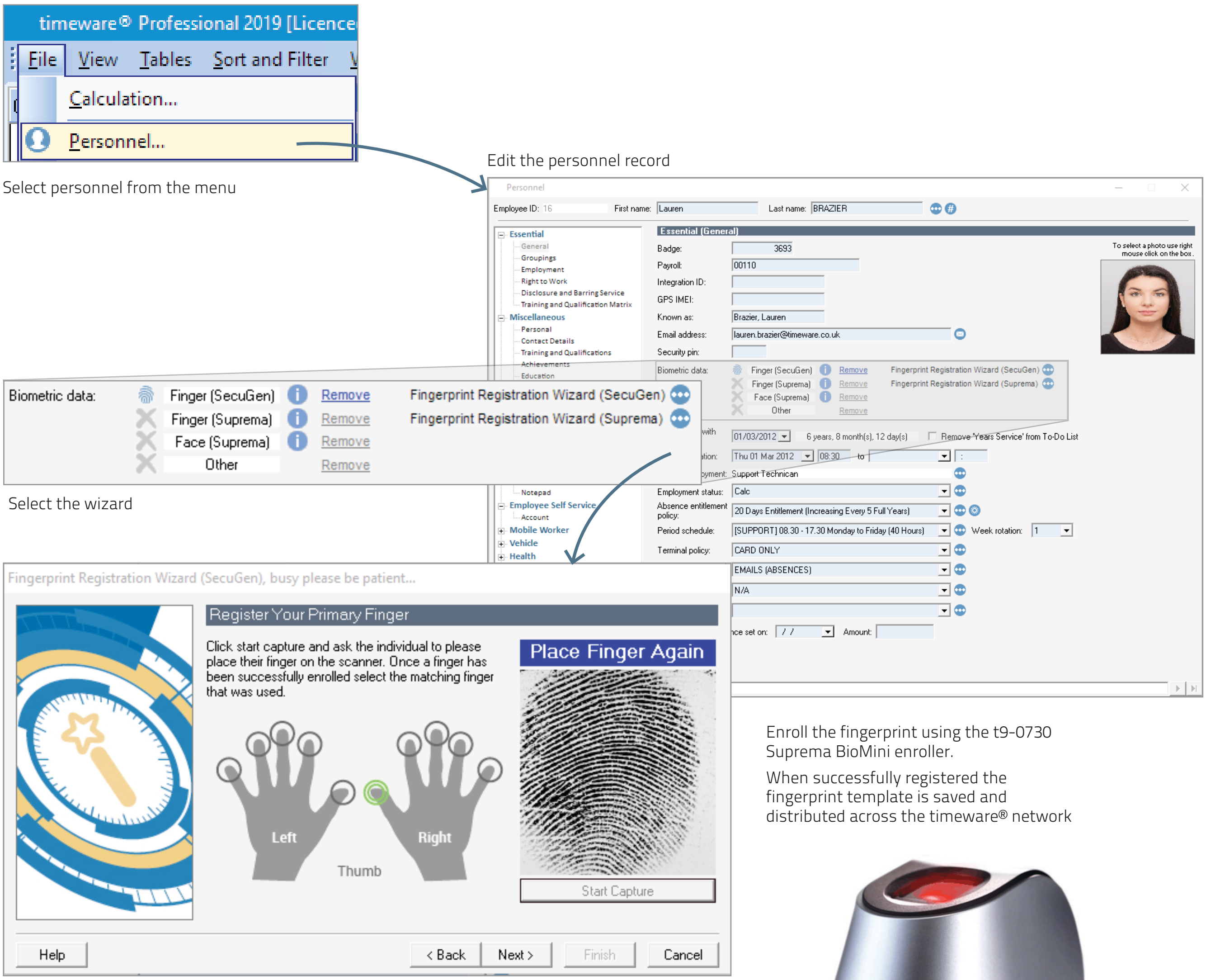


How easy is it to enroll employee biometric data?

An important part of implementing any biometric system is the initial enrolment phase. During this phase, your timeware® project manager will arrange for our support staff to complete the initial bio enrolments of all your employees and agency workers. This process could take several weeks depending on the numbers of staff involved and their work patterns. The support staff will attend site at pre-arranged times of the day to complete the enrolment phase with little or no disturbance to your business. The bio enrolment phase is an essential part of the system implementation plan and your assistance during this process is extremely important..

The timeware® user training covers enrolling new starters via the personnel form utilising either desktop biometric devices or your face recognition device.

Enrolling at the PC – just another small step during the employees induction process.



Select personnel from the menu

Edit the personnel record

Personnel

Employee ID: 16 First name: Lauren Last name: BRAZIER

Essential (General)

Badge: 3693

Payroll: 00110

Integration ID:

GPS IMEI:

Known as: Brazier, Lauren

Email address: lauren.brazier@timeware.co.uk

Security pin:

To select a photo use right mouse click on the box .

Biometric data:

Finger (SecuGen)	Remove	Fingerprint Registration Wizard (SecuGen)
Finger (Suprema)	Remove	Fingerprint Registration Wizard (Suprema)
Face (Suprema)	Remove	
Other	Remove	

with 01/03/2012 6 years, 8 month(s), 12 day(s) ☐ Remove 'Years Service' from To-Do List

ation: Thu 01 Mar 2012 08:30 to :

oyment: Support Technican

Employment status: Calc

Absence entitlement policy: 20 Days Entitlement (Increasing Every 5 Full Years)

Period schedule: [SUPPORT] 08.30 - 17.30 Monday to Friday (40 Hours) Week rotation: 1

Terminal policy: CARD ONLY

EMAILS (ABSENCES)

N/A

nce set on: / / Amount:

Select the wizard

Fingerprint Registration Wizard (SecuGen), busy please be patient...

Register Your Primary Finger

Click start capture and ask the individual to please place their finger on the scanner. Once a finger has been successfully enrolled select the matching finger that was used.

Place Finger Again

Enroll the fingerprint using the t9-0730 Suprema BioMini enroller.

When successfully registered the fingerprint template is saved and distributed across the timeware® network

t9-0730
Suprema BioMini enroller