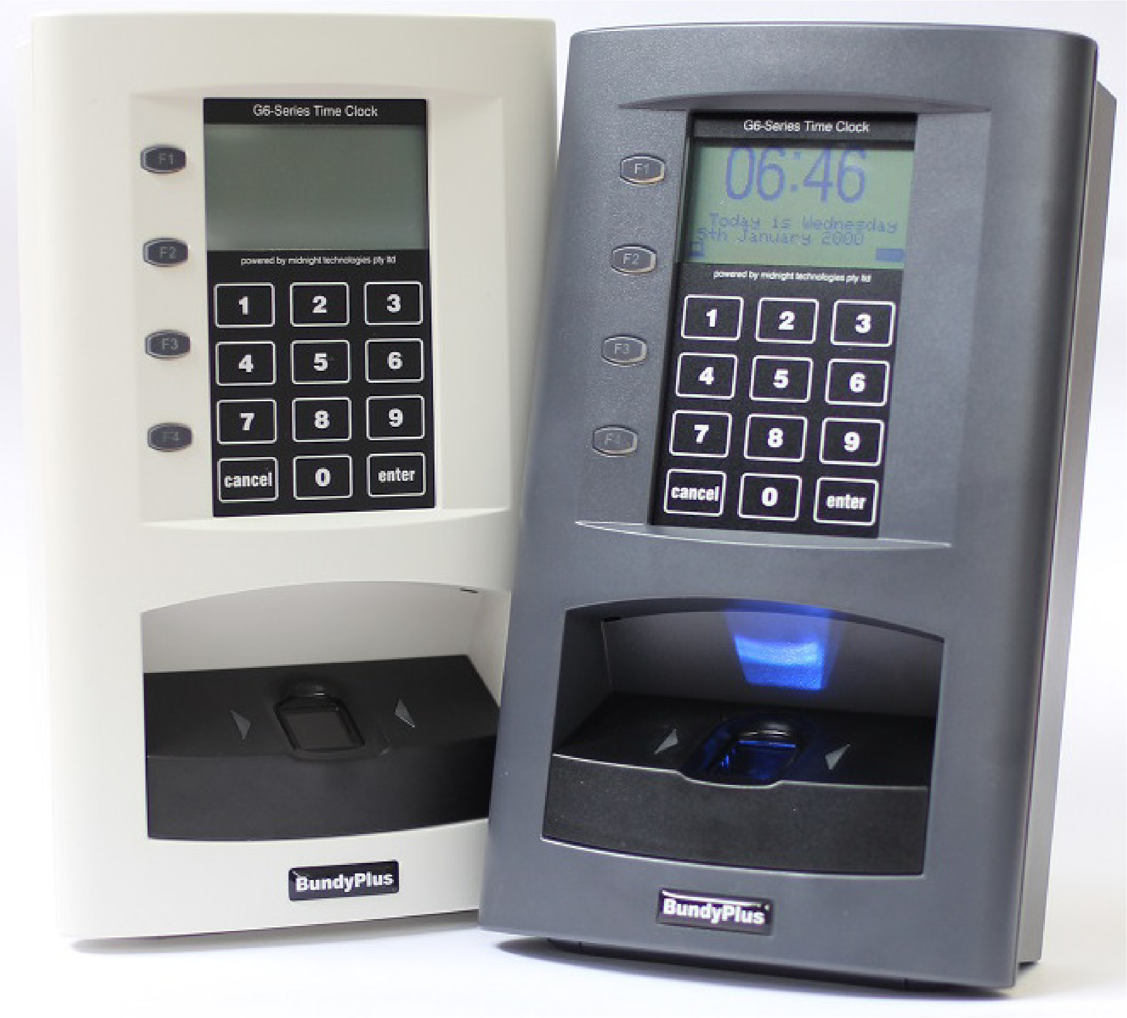
# BundyPlus™

## Biometric Electronic Time Clock



Above shows the G6-BIO-B (Beige case) and the G6-BIO-G (Grey case).

# Table of Contents

# 1. Biometric Concepts

All biometric systems operate on the simple concept of comparing a stored record of a user's biometric data (hand, eye, fingerprint, etc) with data being supplied in real-time by the user requesting access. The real-time data is converted into a form which can be compared to the record, and if the two data sets match with enough certainty, the user is *authenticated*. In Lumidigm's case, the record contains a *mathematical representation* of a fingerprint, which is compared with a *mathematical representation* of a live fingerprint captured from a sensor attached to the device. The process of first capturing the biometric data is called *enrolling* while the action of authenticating the user is called identification or *verification*. During the enrolment process, the original fingerprint image is processed, highly compressed, and stored on the device flash memory (or another storage system like the PC) as a *template* such as a unique ID number, name, and other information is added to associate a person with the template.

## 1.1.Is it possible to trick the sensor?

“Tricking” the sensor virtually impossible, the chances of “tricking” the sensor vary between the different modes supported. Please see “Real-World-Evaluation-Lumidigm.pdf” for the details.

## 1.2.Would a fake finger authenticate?

No! the sensor reads below the surface of the skin to read the live layer, where the true, living fingerprint resides. Because of the approach, anyone who attempts to swipe the finger of a dead person in order to access their important physical or logical data would not succeed.

# 2. Identification verses Verification Modes

## 2.1. Identification (authenticated) - Default

In this mode (default) the employee places their finger onto the sensor – the time clock scans the finger and then searches through the biometric templates to find a match based only on the finger scan. If the employee is found – it will display the employee number or the employee name (if the employee names have been loaded) and ask the employee to confirm that this is the correct employee. The employee answers “Yes” or “No” by pressing any key in the column under the Yes or No prompt. If you intend to use Identification mode we would recommend that you use the authenticated mode as it ensures that the correct employee is recorded.

## 2.2. Identification (un-authenticated)

In this mode the employee places their finger onto the sensor – the time clock scans the finger and then searches through the biometric templates to find a match based only on the finger scan. If the employee is found – it will display the employee number or the employee name (if the employee names have been loaded) and then save this as the clocking. This mode then assumes that the correct employee has been found based only by the biometric scan. We do not recommend this mode for use as it has a higher possibility of identifying the wrong employee.

## 2.3. Verification

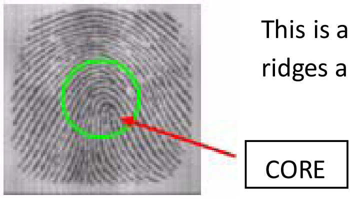
In this mode the employee enters their employee number on the keypad of the time clock, press enter. The clock will then display the employee number or employee name (if the employee names have been loaded) and then prompt the employee to place their finger on the biometric sensor. The time clock will then compare the pre-registered biometric template against the live biometric scan. If the two match then the clocking will be recorded. If the scan does not match then the employee will be prompted to re-scan their finger. Verification mode is a much more reliable mode of scanning as the live biometric scan is only compared against the individual pre-registered biometric template.

## 3. Biometric Performance and Accuracy Parameters

The testing and evaluation of biometric fingerprint technologies are crucial to the success of the deployment. Lack of understanding or information about study design and results commonly leads to an inflated assessment of a system's performance and to invalid comparisons between systems. Thorough evaluation must include "real world" testing and anti-spoof testing. This presentation will focus on the study design and protocols required for the adequate "real world" evaluation of fingerprint technology scanners. It will provide system managers with tools to analyse the important characteristics of a fingerprint scanner.

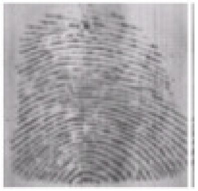
Please see "Real-World-Evaluation-Lumidigm.pdf" for the details

## 4. Examples of Good/Bad Fingerprint Images

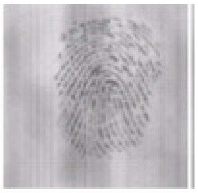


This is an example of a **GOOD** print. Notice that the core is well centred, ridges are well defined and the sensor is covered properly.

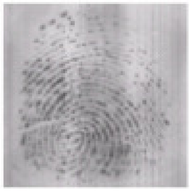
This is an image of the Pinky (little finger). The Pinky is a **BAD** choice to use as a fingerprint since the print is small compared to other fingers. As you can see, very little of the sensor area is covered.



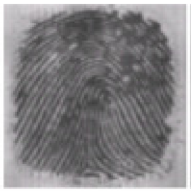
This is an image of the Thumb. The Thumb is also a **BAD** choice for fingerprint enrolment. Although it presents a very large data area, you can see that the core is very low or even non-existent. Do not use a Thumb for enrolment or verification.



This is an example of a user not applying enough pressure. Although the core is centred, you can see that the image coverage is very poor.



This is an example of a **DRY** fingerprint. Notice how the ridge pattern is very light and not well distinguishable.



This is an example of a WET fingerprint. Notice how the ridge pattern blurs into surrounding ridges and the causes problems in the imaging. In this case, dry the finger of the user and retry.

## 5. Privacy Statement

The G6-BIO Biometric time clocks store a mathematical representation of the users fingerprint.  Each time a users finger is scanned by the time clock the mathematical representation of that finger scan is matched against the stored mathematical finger representations which are linked to individual people.

The mathematical representation that is stored with-in the time clock can not be used to copy or re-produce a finger image.

No graphical (bitmap) representation of any finger prints are stored or transmitted.