OVERVIEW

Biometric Authentication

Time & Attendance

What are biometrics?

Biometrics are a new standard to identify employees, focusing on unique physical or behavioural characteristics of individuals, such as their fingerprint or voice.

With biometrics, an organisation knows that an employee is at work, and not just their ID card.

Benefits of biometric authentication:

Convenience for your employees

Remove the need for multiple passwords and swipe cards and makes employee enrolment easier by going directly through the terminal.

Eliminate fraudulent clocking

Ensure the right employee is clocking in at the right time, in the right location.

Enhance your security

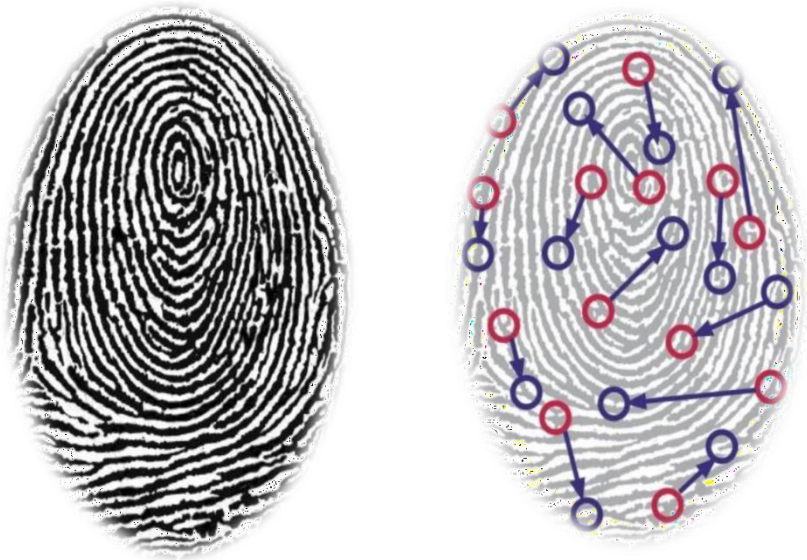
Provide access or entry to controlled areas to employees with the correct identification.

Storing biometric data: Fingerprints

Biometric Template: Normal fingerprint images are too large to store and take too long to process. Biometric authentication use a special algorithm to find unique points on a fingertip (Minutiae).

The coordinates of each Minutiae are stored to form a templates, which is a series of numbers. This biometric template **can not be used to re-create a fingerprint** for identification purposes.

Template Storage: When a finger is present to the clock, a new template is extracted to be compared against the templates stored on the system. At no point is the image of the fingerprint saved, whether enrolled or clocking.



Storing biometric data: Facial Recognition

Biometric Template: The facial recognition process is very similar to the fingerprint recognition. Our software looks for a face in the image from the camera.

When one is detected the same biometrics algorithm reads a set of landmarks on the face, and records their relative position, like the Minutiae on the fingerprint.

Template Storage: These positions form a template which is stored and used in exactly the same way as the fingerprint template.

Storing biometric data: Privacy

Device Storage: The face and finger templates captured are stored in a dedicated encrypted database on the clocking terminal, separate from any other data on the device.

Cloud Storage: whenever the templates are transmitted to and from the web portal, they are encrypted and sent over a secure authenticated connection, and then stored in a fully encrypted database on the cloud.

Image Retention: No finger or face images are ever stored or transmitted by the terminal. It is **not possible to reconstruct a person's fingerprint or face image** from the stored template.

Discover T2 devices

Durable and flexible

T2 devices operate in a wide array of conditions. When dirty environments challenge the fingerprint reader, facial identification can be used as an alternative. Likewise, when lighting or space requirements make face identification difficult, fingerprints can be used instead. Using whichever method is most suitable at each time, **our system allows users to choose facial recognition, fingerprints, or proximity cards** when clocking.

Contact free

The clocking process can be entirely contact free, even wearing a face mask or visor. T2's contactless clocking makes starting and finishing work far more efficient, with the ability to clock in each member of a queue in **less than 5 seconds**.

Connect with us

 +44(0) 330 343 4000

 www.oneadvanced.com

 hello@oneadvanced.com

oneAdvanced