Explaining Biometric Clocking to Employees

Egress Systems Ltd.

Tel: +44 (0)115 931 4007 Web: www.egress-sys.co.uk

Contents

Tel: +44 (0)115 931 4007 Web: www.egress-sys.co.uk

What is Biometric Clocking?

Biometric clocking terminals use detailed measurements of the human body as a means of verifying the identity of the person clocking from amongst the records stored in the clocking device. Clocking on using your hand, fingerprint or facial image is an alternative to using a proximity RFID clocking card or fob, paper punch card or written completion of a timesheet.

To use a biometric clocking terminal your biometric details must first be registered on the device. You will be asked to present your hand, fingerprint or face to the terminal two or more times for your unique details to be recorded. The key details of your biometric profile are stored as a 'template' on the device. These are a series of numbers that record things like the position of the corner of your eyes in relation to the end of your nose or the width of your index finger at various points. Biometric clocking terminals do not record every tiny feature of your hand, fingerprint or face although some models may take your picture for a human to view at a later date.

Once your biometric 'template' has been recorded you can use the clocking terminal to clock on and off. You may need to enter a PIN and in some circumstances use a proximity card before placing your hand or finger on the terminal. When you place your hand or finger on the terminal or stand in front of a face reader the terminal compares your features to either the template associated with your PIN/card or all of the templates stored on the device. If it finds a probable match then the clocking terminal will indicate that you have successfully clocked.

Identification versus Verification

Biometric clocking terminals can be used in two ways. The first is identification ("who is this person?"), in which a subject's identity is determined by comparing a measured biometric against a database of stored records—a one-to-many comparison. The second is verification ("is this person who he claims to be?"), which involves a one-to-one comparison between a measured biometric and one known to come from a particular person. All biometrics can be used for verification, but different kinds of biometric vary in the extent to which they can be used for identification.

Tel: +44 (0)115 931 4007 Web: www.egress-sys.co.uk

Features of Biometric Clocking Types

HandPunch Hand Reader

The HandPunch hand reader only uses the verification method. The user has to enter a PIN to uniquely identify them before their hand is verified against the hand template stored on the system to ensure that they are who they say they are.

The HandPunch uses a camera to view the physical dimensions of a person's hand such as the width, breadth and depth. It does not read the palm print or veins.

Each time the user clocks it will adjust the template stored in the device to take account of weight gain or loss and the addition or subtraction of jewellery.

Suprema Fingerprint Clocking Terminals

Fingerprint clocking terminals rely upon an electronic sensor to capture a digital image of the person's finger print pattern. The terminal converts the fingerprint image into a numeric code which represents relative positions of key features in the fingerprint. These numbers are stored for each user in the clocking terminal and cannot be used to regenerate a fingerprint image.

The clocking terminal may show an image of the user's fingerprint at the time of scanning (depending on the model). This is merely temporarily displayed to provide feedback about the quality of the scan just completed. Neither the clocking terminal nor the associated management software package ever directly store images of a user's fingerprint.

Fingerprint clocking terminals can be configured to use either the identification or verification method for clocking.

Face Readers

Face readers invariably use the identification method where no touching of the machine is required at all for clocking. When a face is presented in front of the terminal the terminal will attempt to match that face to its stored face templates.

Face readers record the relative positions of the core features of your face when creating the template for storage. You may need to remove your glasses when using a face reader.

Tel: +44 (0)115 931 4007 Web: www.egress-sys.co.uk

The Advantages of Biometric Clocking

Preventing Timesheet Fraud

The primary purpose of biometric clocking terminals is to eliminate timesheet fraud. That is, preventing employees from falsifying their timesheets or clocking their colleagues in and out on their behalf ("buddy clocking").

Businesses with high turnovers of temporary staff are particularly susceptible to "buddy clocking" as are organisations where staff are not closely supervised or do not follow a regular shift pattern. The practise of "buddy clocking" is widespread enabling some individuals to hold multiple jobs but only turn up for one shift while their "buddy" clocks them in and out as if they had been at work for the day. This not only defrauds the organisation involved but also other workers who could have legitimately held employment. In the public and outsourcing sectors this is defrauding the tax payer. Even when "buddy clocking" involves the loss of half an hour's work a day this could add up to over 100 hours of lost time and fraudulently claimed pay over a year.

Preventing Employee Impersonation

Biometric clocking terminals can provide confidence for the employer, staff and members of the public utilising an organisation's services that the correctly trained and insured individual has attended for work. Ensuring that the correct person attends work can be essential in some specialist jobs where employees are skilled, working with vulnerable people, working alone or with unfamiliar colleagues. This could be a matter of health and safety and is an important duty of employers to attend to.

Security

Many biometric clocking terminals, such as the Suprema Biolite Net, can also be used for access control installations on doors, turnstiles and barriers. Consequently they can provide enhanced security for the business and other employees by only allowing verified staff to enter the premises or secure areas. Proximity cards are easily lost or stolen. Therefore, if they fall into the wrong hands not only would security be compromised but employees could inadvertently find that it was their card that had been used to gain entry, potentially making them a suspect in any crime.

No Lost or Damaged Clock Cards

Most biometric clocking terminal installations do not require the use of a clock card and consequently biometric devices can eliminate missing clockings due to lost or damaged clocking cards or fobs.

Accurate Fire Muster Reporting

By eliminating "buddy clocking", employee impersonation and missed clockings due to lost or damaged cards fire muster reports produced by the Focus Time & Attendance software will be more accurate and reliable.

Tel: +44 (0)115 931 4007 Web: www.egress-sys.co.uk

In the event of a fire or other life threatening emergency, such as the escape of noxious fumes, muster reports can be essential for identifying missing individuals who need to be accounted for. Fire fighters will no longer need to risk their lives searching for people who were never actually on the premises because their colleague fraudulently clocked them on. People won't be forgotten who failed to clock on because of a missing clock card (although they may still forget to clock) and confusion will not reign as a result of impersonation.

Limiting Tribunals & Overheads

Providing a deterrent for employees intent on fraud, and preventing them from committing it, not only limits the loss of money that they fraudulently claimed. Biometric clocking systems result in significantly less time and money being wasted on checking the accuracy of timesheets, pursuing fraudsters and taking disciplinary action for supervisors, managers and HR staff.

They can also benefit unions by minimising tribunals associated with dismissals concerning timesheet fraud, which are costly and take away resources available to other members. Accurate, valid and verified clocking records can also help unions mount a valid defence of employees who feel that they have been unfairly dismissed, without the organisation being able to claim timesheet fraud may have been a factor in a good clocking record.

Tel: +44 (0)115 931 4007 Web: www.egress-sys.co.uk

The Disadvantages of Biometric Clocking

There are some disadvantages to biometric clocking that it is wise to be aware of.

Firstly, when introducing a new biometric clocking system staff are bound to be worried and may be offended at the thought that their biometric data is being recorded. They may feel that enrolling their hand, fingerprint or face on a biometric clocking terminal is an invasion of their privacy and feel affronted. They may also misunderstand how the technology works or fear that their biometric data could be used for malicious or underhand purposes.

How an organisation approaches the installation of a new biometric clocking system is consequently crucial. It is important to provide employees with accurate factual information about the chosen system and address commonly held concerns early in the process. A culture of transparency and openness should help dissipate "Big Brother" fears. Further down this document is a selection of commonly voiced concerns and some mitigating responses.

Each type of biometric clocking terminal has its own advantages and disadvantages which mean that choosing the appropriate clocking terminal for the environment and organisation in which it is deployed is vital.

HandPunch Hand Readers

HandPunch hand readers are accurate and robust in just about every setting but cannot be located outside without a shelter, rain cover and heating.

Hand readers need regular cleaning and calibration to ensure that accuracy is maintained. Over time dirt and use will affect the quality of the templates stored on the clocking terminal. When properly maintained a hand reader will perform accurately for many years without performance problems.

The HandPunch hand reader requires the use of the right hand and all five digits need to be present. To mitigate this it is possible to use the "Special Enrol" feature that allows an individual to clock in and out even when some of their digits are missing. In the event that an employee cannot use their right hand the left hand can be used upside down.

Suprema Fingerprint Readers

Suprema fingerprint readers use market leading algorithms for matching fingerprints to templates and have a very high degree of accuracy. They are also better than many other fingerprint terminals available at recognising the small percentage of the population who have fingerprints that are indistinct due to generic characteristics, wear and manual work. However, there will still be the occasional employee whose fingerprint cannot be registered on the clocking terminal and will need to use an alternative clocking method.

Fingerprints will be affected by cuts and abrasions so fingerprint readers are generally unsuitable for heavy industry or food preparation areas but can be ideal for warm, dry, clean environments. Waterproof fingerprint terminals are available for outside use. It is normal to enrol two fingers for each employee to cater for situations where there has been injury to the primary finger.

Tel: +44 (0)115 931 4007 Web: www.egress-sys.co.uk

Face Readers

Face readers need to be sited out of direct sunlight as this can affect their ability to 'see' a face in front of them (just as we struggle to see when a light is shining in our eyes).

Employees may also have to remove their glasses when registering on the clocking terminal and clocking. It may be possible to register on the clocking terminal whilst wearing glasses but the face reader would be unlikely to recognise an employee if they changed their glasses.

Tel: +44 (0)115 931 4007 Web: www.egress-sys.co.uk

Common Workforce Concerns

Is my personal biometric data secure?

The templates that are recorded by the biometric clocking terminal are extracted by the time & attendance software and held in a database. They can also be transferred between clocking terminals of the same type through the software. The clocking terminal, software, database, computers and network on which they run all have their own security systems. Like any electronic or computer system they could, in theory, be hacked if a competent hacker was intent on doing so. Even the Pentagon is successfully hacked from time to time.

However, if these devices were hacked the information recorded could not be used to recreate your fingerprint, handprint or facial image. All that is recorded is a series of numbers relating to a limited number of key elements of your biometric data that are used by computer algorithms to determine a probable match to the fingerprint / handprint / facial image captured by the clocking terminal. The fingerprint that you left on the coffee cup you just drank from will contain more valuable information about your identify that the clocking terminal.

Could the police (or anybody else) obtain my biometric information if they wanted to?

There is nothing useful in the biometric template stored in the clocking terminal or in the database that would help the police with their investigations. However, the police may be interested to obtain records of your clocking history to verify your attendance at work as they might do with any clocking system, CCTV recording or timesheet record to assist a crime investigation. The fact that biometric clocking terminals are used would make that information more reliable than conventional clocking data.

My twin/sibling works here too. Will we have the same biometric information?

No. Your biometric information will not be identical but it could be similar. In rare circumstances it is possible for a clocking terminal to fail to match because templates are too similar to each other and it cannot choose between them when trying to establish identity from its known templates. This is normally caused by a poor quality template. Re-registering the biometric information should resolve the problem. If it doesn't, changing the tolerance levels may help or using a one-to-one verification method of clocking instead (where a PIN or clock card is required as well).

Can I be made to surrender my biometric information against my will for the purposes of clocking in and out?

This may form your new terms of employment. Consult your HR department for more information.

Are you using this system to control everyone?

Employees will be expected to attend work according to their contracts of employment exactly the same as they were before. The only difference is that you are being asked to use a biometric clocking device to accurately record your attendance. This system is to the advantage of everybody

Tel: +44 (0)115 931 4007 Web: www.egress-sys.co.uk

as you will be able to demonstrate your commitment to the job and additional time worked just as the management will be able to identify non-attendance and lateness.

The organisation wants to ensure that no-one is clocked on and off by someone else – that means you don't trust your employees. This is the equivalent of calling us cheats and thieves without evidence.

Unfortunately, although you may be a trustworthy individual and so are most of your colleagues not everybody is. By no means does everybody abuse the system and the vast majority of employees are extremely conscientious about only claiming what it due to them. There are however, a few individuals who exploit the system and claim hours that they have not worked. This is unfair not only for the organisation but also for all those that work hard for their living.

Can it read my DNA?

No. DNA is held within your body tissue, hair, teeth and bodily fluids. These are not captured, read or recorded by the clocking terminal.

Touching the machine is unhygienic and will spread germs and diseases.

It is true that germs and viruses can be spread when people touch the same object if germs or viruses are present on their hands. The risk of using a fingerprint or hand reader, however, is no greater than using a door handle. To mitigate any risks organisations can make hand washing facilities available or provide sanitary wipes for use after clocking (please note that use of alcohol gels prior to clocking can damage the equipment).

What if the machine malfunctions? The employer will believe the "infallible" technology rather than me.

Machines do go wrong from time to time and biometric clocking terminals are no exception. Regular cleaning, maintenance and calibration of the clocking terminal should minimise any failure. Occasionally, biometric clocking terminals will fail to recognise a legitimate employee due to a poor quality template or changing environmental conditions. These problems can normally be resolved by changing the configuration settings in the terminal, re-registering the biometric template or very occasionally an individual employee may need to use a PIN and password or proximity clock card instead of their biometric data to clock. Any suspected failures of the equipment can be investigated by Egress Systems, under a hardware support contract, or the manufacturer.

"We believe this technology infringes on staff civil liberties", Bob Crow, RMT union general secretary

Civil liberties are the basic rights and freedoms granted to citizens of a country through national common or statute law. For example: the freedom of movement. Biometric clocking systems do not prevent you from moving about your business freely, they simply record when you clocked on and clocked off work.

By 'civil liberties' some people might mean their privacy, and feel that divulging their biometric data to a machine may infringe that. However, in reality none of the biometric data recorded and stored

Tel: +44 (0)115 931 4007 Web: www.egress-sys.co.uk

by the clocking terminal is capable of being used by government or law enforcement agencies. The data simply isn't detailed enough and your actual fingerprint, hand dimensions or facial image cannot be recreated from the information stored. The reason biometric clocking works is that your biometric data is only being compared to a very small number of people – the few people that work for the same organisation as you – and in many cases it is only being compared to one stored template, the one you recorded in the first place. The technology simply isn't capable of matching your details against the whole population, even if such a database existed.

You're treating us like slabs of meat. This infringes our dignity.

It is not undignified to have your picture taken for your bus pass, enabling the bus driver to check that you are the real holder of the ticket. So why should it be undignified to have a record of your hand, fingerprint or face taken to check that you are the real employee turning up for work?

There is a stigma attached to the taking of fingerprints in particular because of their use for over 100 years in forensic investigations by the police, but having your fingerprint taken does not make you a criminal. Homeowners routinely have their fingerprints taken when they are victims of a burglary to separate their fingerprints from ones that could have come from the burglar. Employees using a fingerprint clocking terminal won't even be having their fingerprint taken, in the traditional sense, because there will be no record of the unique loops, arcs and whorls that make them an individual, only a numeric code representing those features. This can never be used to recreate their fingerprint.

What happens if I can't clock on because I cut my finger / break my arm?

Fingerprint clocking terminals often require the registration of more than one fingerprint so that an alternative finger can be used for clocking in the event of a cut or abrasion. If this is not the case an alternative finger could be registered on request to your supervisor.

Likewise, if you are unable to use a HandPunch clocking terminal temporary alternative arrangements can be made to use your left hand for clocking or for you to use the special enrolment function.

What happens if I lose or gain weight?

This will be no problem if you use a face or fingerprint reader as the position of your facial characteristics will not change or your fingerprint.

When you use a HandPunch clocking terminal the terminal updates the template it has stored in the device each time you use it so gradual changes to the shape of a hand will be recorded.

It feels like 'Big Brother' is watching us.

Clocking systems, whether biometric or not, are not designed to capture an employees every movement. Instead they are designed to determine the correct times an employee started and finished work for the purposes of calculating pay and identifying lateness and absence. Using biometric clocking terminals is a more accurate and efficient method of capturing this information

Tel: +44 (0)115 931 4007 Web: www.egress-sys.co.uk

than manual methods. Biometric clocking systems ensure fairness and consistency by using real data rather than approximations.

Further Reading

Article in The Economist, *Prepare to be scanned*, Technology Quarterly: Q4 2003, 4th December 2003
http://www.economist.com/node/2246191

Article in HR Magazine, *Are you ready for Biometrics?*, Volume 48, no. 3, by Bill Roberts, 3rd January 2003
http://www.shrm.org/publications/hrmagazine/editorialcontent/pages/0303hrtech.aspx

BBC News Technology Article, *Tube cleaners refuse fingerprint clock-in, union says*, 16th September 2013
http://www.bbc.co.uk/news/technology-24117006

Tel: +44 (0)115 931 4007 Web: www.egress-sys.co.uk