



Electrone Biometrics Opinion

The Biometric bandwagon and getting hitched to it

Biometric technology offers the potential of a plethora of benefits to businesses and individuals alike – safer sales transactions, no need for a wallet full of plastic cards and easily forgettable passwords, even the eradication of identity theft. But there is a huge potential for businesses to run themselves into technology 'blind alleys' and future-proofing these systems will pose many challenges for the industry, says **Stuart Thorn, Chief Executive of Electrone Europe.**

Today there's a range of questions that anyone considering a biometric system must give serious thought to consider. Health and safety, privacy and security - all must be examined carefully when selecting a new system. These are the issues that will grab the headlines for all the wrong reasons if everything goes wrong.

However, it's all too easy to let these often hyped concerns cloud some of the difficulties inherent in all biometric technology – problems which, if not considered from the outset, may have serious financial implications in the future.

Health and safety

Throughout the development, testing and roll-out phases of biometric systems there have been worries about the health and safety issues of the equipment that will sample and capture the biometric data. Branded as invasive devices by consumers, retinal scanners have particularly suffered despite the fact that no physical contact needs to be made.

This technology requires a close encounter with a scanning device that sends a beam of light deep inside the eye to capture an image of the retina. Concerns over infection, although unwarranted, combined with common phobias related to the eye, have limited major take-up of such schemes.

Scanning of the iris, the unique coloured ring that surrounds the pupil in your eye, is much less intrusive, but the subtle distinction has been a hard sell in some quarters.

However, the Home Office's Iris Recognition Immigration System (IRIS) was extended to Gatwick Airport's South Terminal in May – the ninth UK airport to adopt the scheme. Many pairs of eyes will be watching this project as iris recognition, still a relatively new science, is put firmly in the spotlight.

Another possibility lies in palm print biometrics. These scanners look below the surface of the skin and analyse blood vessel patterns. This may be great 'sci-fi' technology but examining these unique patterns can come at a hefty price.

Why would you pay ten times the amount you would on fingerprint technology for just one percent of extra certainty?

Looking for the future of biometrics in palms is therefore likely to prove unjustifiably expensive. It's therefore surely fingerprint technology that is by far the easiest system of choice for widespread and economical implementation.

But the above difficulties of some biometric systems are just scratching the surface of the underlying issues in the software technology which underpins the equipment – the databases and algorithms which store and manage the data for the company operating it. If you consider that five different biometric readers could record five completely different versions of your fingerprint/retina/iris – in different formats, with differing amounts of data.

As a result, if sometime later you want to change or upgrade the hardware it may not operate with the same 'digitising algorithm'. The result is that expanding your system in the future or merging your company with another could see you are locked in to the technology you chose first and could pose significant problems of interoperability between merged systems. It's this issue which anyone considering a biometric system needs to examine carefully before rushing headlong down an expensive dead-end.

Interoperability

The industry has failed to both highlight and attempt to tackle these problems with vendors preferring instead to promote their own proprietary solutions. This problem may also spread to non-biometric solutions recently implemented by some the UK's largest banks. Both Barclays and the Royal Bank of Scotland are

dishing out smart-card readers to customers aiming to reduce online banking fraud.

However, whilst excellent in theory, there are questions over how practical these authentication devices may be in reality. Many customers have multiple accounts with different high street banks. How many different devices from different banks cluttering up their desks and home will customers put up with?

The continued lack of interoperability has slowed down development and extensive adoption of biometric systems and also could effect Chip and Pin in the home. There is a new generation of sophisticated and affordable pin pads, biometric readers and scanners available which have multiple compatibilities and can be integrated into keyboards. Banks need to be looking ahead now to assess the usability of this new technology.

The solution for biometric devices could be found in translation 'middleware' software. However, translations are extremely complicated and can involve simultaneously searching multiple, possibly very large, identification databases. This search can require a huge amount of processing time which would be at odds with, say a fingerprint scanner at an airport check-in desk hoping to cut long queues.

Intelligent searching can help to an extent. Simple flags, such as finger size, can be used to quickly rule out many possible matches. However, combining the fingerprint system with a secondary authentication device, such as a pin number, can ease the problem of database searching. Pin data can identify users instantly, leaving the fingerprint reader to simply match the cardholder's identity. Verification rather than identification is surely the way forward for such systems.

Co-operation over standardisation

One initiative in particular brings fresh hope to those hoping to encourage the greater use of biometrics across all areas of industry. April saw the formation of the United Kingdom Biometrics Institute – a concerted effort by the University of Kent's Department of Electronics and Kent Enterprise. The UKBI aims to enhance the knowledge exchange between researchers, industry experts and potential end-users and hopes to be seen internationally as the voice of

biometrics in the UK.

Some may hope the UKBI will help develop biometric standardisation but in reality it is greater co-operation that is needed. Standardisation will not only meet resistance from the outset but the security implications of such a move could undermine the whole biometric process. Common open architecture digitising algorithms could be left useless if criminals find weaknesses in encryption techniques. This problem, already present in the adoption of wi-fi, would surely be best avoided. Secure proprietary digitising algorithms working together in open databases, forged on industry co-operation, are the way to empower the industry.

Resellers and systems integrators must take great care not to jump hastily onto the biometric bandwagon and make the technology choices quickly on 'look' and 'feel' alone. They must remember that different methods are employed to store biometric data and a number of disparate search algorithms used to access it. Just a couple of years after implementing a piece of biometric technology you may wish to add more features or use different scanning hardware. This could have different algorithms and now the two databases really are like two different languages and do not talk to each other.

There is a risk of becoming 'wedded' to the technology chosen at the outset. Wise folk have said 'Marry in haste, repent at leisure!' – it may be hard to undo the decisions taken at the outset of the venture!

ENDS