



Biometrics: time to evangelise the benefits

Biometrics technology – and the security surrounding it – has moved on, making it a feasible solution for many risk management and security applications. But first, senior stakeholders need to be convinced that it is really worth the investment.

Biometrics have been used to verify people's identity for thousands of years: beginning with very primitive systems in ancient Egypt 'when records of distinguishing features and bodily measurements were used to make sure that people were who they claimed to be'¹. Today, 'biometric hand and iris scanners are being used regularly in the UK for workers to access high profile, sensitive, construction sites as part of developers' measures to enhance safety and security on site'².

Some recent implementations have been problematic, to the extent that, today, the objections to biometrics are more widely understood than the benefits. However, technological advances in the past decade mean that biometrics are now ripe for re-evaluation by the Chief Information Officer (CIO) community.

Already there are working applications, such as the use of fingerprint readers to restrict access to secure zones in some sophisticated data centres and the Citibank 'cardless biometric payment service'³. Trials have proved that it's possible to utilise facial recognition technology, linked to boarding cards, to distinguish between domestic and international travellers at airports⁴.

If CIOs want to initiate, deliver and sustain biometrics-enabled identity management systems, their main challenge lies in convincing stakeholders of the benefits.

¹ *The measure of man, The Economist, 7 September 2011.*

² *Biometric scanners enhance Olympic Park security as big build ramps up, London 2012, 16 October 2009.*

³ *Citibank launches world's first cardless biometric payment service with the new clear platinum card, Citibank, 8 November 2006.*

⁴ *Upgraded biometric passenger scans at Heathrow, Airport International, 26 July 2011.*

Why consider biometrics now?

Identity fraud is widespread, and ranges from theft of credit card information to falsification of identity documents to obtain credit in someone else's name. Such fraud will continue to grow if left unchecked. In the UK alone, CIFAS (Credit Industry Fraud Avoidance System) and SOCA (Serious Organised Crime Agency) have estimated that identity fraud costs the UK economy more than £1bn per annum. The true figure may be much higher.

The UK abandoned the national identity card programme, as well as a proposed second generation of biometric passports, in 2010, primarily on the grounds of cost and the lack of a clear benefits case. We believe that this was a missed opportunity for the UK to improve its reputation for holding citizen data securely, and to enable government services to be delivered more effectively and efficiently.

A recent Ernst & Young publication⁵ said that 'organisations that ignore the importance of protecting personal information from outside – or inside – [threats] will suffer more than financial penalties. They may also see their reputation damaged and their brand negatively impacted'. This should be a wake-up call to buyers, sellers, consumers and delivery agents that it's time to promote the benefits of biometrics-enabled identity management systems because biometric recognition can provide a strong link between an individual and a claimed identity. The technology can help guard against attempts to establish fraudulent multiple identities, and can prevent identity fraud. By means of a search through stored references, individuals who appear to have previously enrolled using a different identity can be highlighted for further investigation. This cannot be done without biometrics.

Biometrics, when implemented correctly and appropriately, can enhance the customers' experience by making identity checks faster, more convenient and more secure. For example:

- ▶ At entry points to some countries such as the UK, 'accredited customers'⁶ can pass through automated gates rather than stand in a potentially longer queue to have their identity documents inspected.
- ▶ Belgium allows its citizens to establish their identity almost instantly when using any of 100-plus government services (including voting). There, and in other countries with national identity schemes, there's no longer any need to carry paper documents to prove identity. Some of these countries would like to allow business to use the same infrastructure to reduce fraud, with the potential upside of boosting their economies.

Biometrics applications

Biometrics-enabled identity management systems can be used to deliver services at lower cost and reduce the risk to which both public and private sector expose themselves when interacting with other parties. Situations where biometrics could help, or are already helping, include the following.

- ▶ Governments around the world face the twin challenges of controlling net migration and keeping undesirable characters out. In recent years, some governments have moved to integrate their border control and intelligence systems, and, by adding biometrics, create a more effective and less costly solution to controlling migration.
- ▶ In recent years, there has been a surge in the circulation of fraudulently-obtained but genuine documents – that

is to say the document is genuine but false details have been added. For example it was widely reported in the UK⁷ and international⁸ press that the Israeli spies who entered the United Arab Emirates in 2009 to kill a member of Hamas used fraudulently-obtained passports. If all border controls had implemented the latest International Civil Aviation Organization (ICAO) guidance on machine-readable travel documents⁹, these spies would not have gained legal entry to the country, because the images stored on the passport chips would not have matched the live images captured at border control.

- ▶ The banking industry and those it interacts with are particularly vulnerable to fraud. Having already taken steps to reduce card fraud in the last decade, the banking industry is now moving towards the use of voice recognition systems to verify that the customer speaking to the bank when not physically present is who they say they are. Implementation of such technology will reduce operational cost and improve the industry's reputation.
- ▶ Retailers in the developed countries prefer to receive regular electronic payments for an ongoing service rather than collect cash. Their challenge is to be sure that a consumer to whom they're granting credit is who they claim to be. Retailers in some countries use identity documents to reduce this risk, but a more integrated system will no doubt improve the experience that they offer their customers.

⁵ *Privacy trends 2011, Ernst & Young*

⁶ *Typically, customers must pre-enrol to allow access to automated gates.*

⁷ *Times online, 16 February 2010.*

⁸ *Washington Post, 18 February 2010.*

⁹ *ICAO MRTD website.*

Dealing with the objections to biometrics

It would be naive to assume that stakeholders will forget all their fears surrounding biometrics. The kind of myths shown in the table below can be very compelling, and without having given the matter much thought people can easily believe them. For example, is it really true that identical twins can fool an identity management system? Easy to believe – but in reality the vendors have resolved this problem to the extent that the system can spot the difference, or at least flag that it cannot: in the latter case a highly experienced human can then review the biometric sample.

Can criminals really chop your finger off and use it as a biometric sample? No. This is not the movies. 'Liveness' detection of the biometric sample has been introduced to biometric systems in recent years to combat this potential weakness.

The way forward

In 2010, Ernst & Young published an article, *Biometrics: primed for business use*¹⁰, in which we proposed three models to deliver biometrics-enabled identity management systems. We believe that these models are still valid, but within some countries there is a specific lack of trust in government to hold citizens' sensitive biometric data and to deliver complex programmes. We now believe that the next growth area will be in industry-centric programmes and, where appropriate, in organisation-specific programmes.

Industries such as banking or credit reference agencies are well placed to act as custodians of biographic and biometric data. An industry-wide solution could also allow citizens to share their data with government-provided services: for example, to confirm that they are entitled to claim child benefit. Some organisations can make a business case for implementing biometric-enabled identity management solutions, particularly for access control.

Ultimately, we believe that all programmes need to evangelise the benefits, obtain buy-in, incentivise stakeholders and commit to landmark dates if they are to deliver a successful identity management system.

Evangelise the benefits – the benefits case needs to be tangible and easily understood. It is vitally important to engage customers and other stakeholders in order to build confidence in the system, to obtain buy-in and to manage expectations (including dealing with those myths).

Obtain buy-in – biometrics-enabled identity management systems are not widely understood. Therefore, to obtain the organisation's commitment, it's worth showcasing the technology to decision makers, and selecting a business owner as your programme sponsor. The major challenge will be to balance the divergent goals of the stakeholders.

Incentivise stakeholders – the vendor and advisory market is maturing, but as well as choosing the right partner for your programme, consider incentivising them to deliver a successful system with you. After the system is launched, these providers can help your business stakeholders to ensure that the system is not fully under utilised.

Commit to landmark dates – implementing this type of system is complex, particularly in the areas of requirements elaboration, testing and change management, because

you're dealing with probabilities rather than certainties. Nonetheless, to focus stakeholder minds, it's vital that the programme commits to critical milestone dates to keep the programme on track.

Conclusion

There is a bright future for biometrics-enabled identity management systems. Identity fraud is a growing problem; if left unchecked, it will spiral out of control. We believe that the appropriate use of biometrics can offer significant benefits to government, business and consumers. The biggest challenge for CIOs needing to ensure a successful biometrics programme is to convince the rest of the organisation of the benefits.

What are biometrics?

A biometric can be defined as ... "a trait of a human being that can be used to identify them uniquely"¹¹.

Biometrics currently in use include facial recognition, fingerprints, signature, iris, voice recognition, vein pattern recognition and palm geometry. Further biometrics are emerging or possible: these include keystroke analysis and gait analysis.

Dispelling some myths about biometrics

Myth: iris recognition devices use lasers to scan your eyes.

Reality: iris recognition cameras take a black and white picture and use non-invasive, near-infrared illumination that is barely visible and very safe.

Myth: 'stolen' body parts can be used to fool the system.

Reality: quality biometric recording and detection systems can determine 'liveness' in order to prevent this type of fraud.

Myth: identical twins can fool the system.

Reality: if the system is poorly configured, then this is possible (but should be eradicated during testing). Good systems will highlight a false match, which will require human intervention to complete the identification process.

Myth: biometrics will get rid of the evil in our world.

Reality: identity management systems cannot perform miracles.

¹⁰ Available from: <http://performance.ey.com/2010/07/16/biometrics-primed-for-business-use/>

¹¹ Ernst & Young definition.

Contacts:

Stephen Davies

+44 (0)20 7951 3133

sdavies5@uk.ey.com

Sean Meade

+44 (0)20 7951 6819

smeade@uk.ey.com

Ernst & Young LLP

Assurance | Tax | Transactions | Advisory

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place,
London, SE1 2AF.

© Ernst & Young LLP 2011. Published in the UK.
All Rights Reserved.



In line with Ernst & Young's commitment to minimise its impact on the environment, this document has been printed on paper with a high recycled content.

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young LLP accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

www.ey.com/uk

1142593.indd (UK) 10/11. Creative Services Group.