A question of identity

John Dale, managing director of KeCrypt Systems, puts forward his argument as to why dynamic signature verification technology should be included in national ID card schemes, such as that being proposed in the UK.

Life used to be so simple. All it took to authorise a payment, confirm agreement to a contract, or validate receipt of goods, payment or service, was your signature. At a stroke it confirms intent and is integral to the legal process. A signature is the simplest, most familiar and authoritative way of signifying agreement and approval – and virtually everyone can do it.

You are not a number

We make do with passwords and PINs for identity in electronic processes, and even authentication of transactions, but they don't identify anyone. They are forgotten, given away, obtained by deception and violence.

So increasingly the search for a way to irrefutably establish identity has focused on biometrics. The choice of biometric has been mainly driven by the standards set by the International Civil Aviation Organisation (IACO), set up in 1944 by the United Nations to promote safe international civil aviation.

ICAO decided to adopt a biometric scheme for machine-readable passports involving facial recognition, optionally supported by fingerprints and iris recognition. These are the biometrics (not iris recognition) that are being included in the chip-based passports now being issued by the UK, and increasingly in other countries worldwide. As a result it is often only these biometrics that get considered for other forms of personal identification, such as visas, national ID cards, international citizen cards, driving licenses, government workers, seafarers and so on.

The ICAO standard appears to have blinkered system designers in their choice of biometric modalities.

To sign over, sign here.

There is an interesting irony in all this, however. In the process of ID card registration individuals have to authorise the handing over of these other biometrics by signing, because *only* their signature has the legal status to enable this. Even the issuing authorities concede that only a signature demonstrates intent and has the unique quality of inherent non-repudiation.

So if only a signature will authorise the taking of other biometrics for an ID, then logically the dynamic signature biometric should be included on the card.

UK ID Card lacks user appeal

A case in point is the proposed UK ID card. It will have facial and fingerprint biometrics, which are essential for its use as an EU travel document that removes the need to carry a passport. Both these biometrics are also essential if the authorities wish to check criminal databases. However, it's precisely because of the adverse social connotations of these checks that the public are reluctant to use facial recognition and fingerprints for other interactions with the government or commercial organisations.

It has already been established that the signature is still required for legal transactions. If the dynamic signature biometric is not part of the ID card then even if it is used in a legal process to provide legal intent, the binding between the identification proven by the biometrics on the ID card and the real-time signature used in the transaction is lost.

So why not also include the dynamic signature biometric on the card?

Qui Bono – who benefits?

If the UK's national ID card is going to be a legal requirement, it's surely appropriate to apply legal strictures to it. One important principle is to ask who benefits from it.

It's very easy to envisage the many citizen/government interactions that are simplified and protected against fraud by the use of secure identification. Uses by Social Services, the Inland Revenue and Local Authorities are obvious examples. However, if citizens have to continue to carry additional forms of ID for commercial use; for example two utility bills with name and address; then the benefit of the National ID card appears biased towards the government and not the individual.

To be a benefit when setting up a bank account or agreeing a contract, the National ID card needs to be universally accepted across government and commercial sectors. Not surprisingly, the majority of people would not trust commercial business with access to the government database holding their biometric data.

Look what happened to card PINs when access was increased from the 57,000 secure ATMs to the many hundreds of thousands of retail outlets. This increased exposure was exploited by criminals, PINs were compromised and customers suffered.

Would this happen with government held biometrics? Probably not, but perception is everything – especially when it comes to personal privacy.

Signing off

The simple, obvious solution is to include dynamic signature verification – the most user-acceptable form of biometric identification - on the card. The cardholder's signature, held in a form that's impossible to forge, can then be verified on the card with a simple writing tablet (as used in many US retail stores today) without the need to interrogate a central government database.

Such a card would be equally acceptable to citizens, government and commercial users for the purposes of authentication. A signature biometric will remain the most natural, acceptable and secure way to demonstrate legal intent and provide non-repudiation. Unlike other biometrics, the physical act of signing provides a unique sense of closure and commitment to every transaction that involves an ID card.

This opinion piece was contributed by John Dale, managing director of KeCrypt Systems, web: www.kecrypt.com