ID Cards and the National Identity Register

Professor Paul Wiles, Chief Scientific Advisor, Home Office

Introduction

The UK plans to move to the introduction of ID cards and the creation of the National Identity Register, subject to Parliamentary decision, with the aims of reducing the opportunity for ID theft, simplifying immigration procedures and supporting stronger verification of identity in the use of public and commercial services, both on- and off-line.

ID cards are not a new concept; indeed an ID card was introduced in the UK during the Second World War, and most EU countries have them. However, better ways of securing the card, both when issued and in use, are needed. Biometric technologies are already used with identity cards for these purposes in other countries such as Malaysia and Hong Kong. Also, ID cards using international standards are becoming available for the first time, and the proposed UK identity card could benefit from these and the experience of other countries.

The key components of the proposed ID cards scheme include:

i) a strong enrolment process to ensure that the credentials supplied by the applicant have been checked thoroughly and that he or she has not attempted to enrol previously;

ii) the creation of a National Identity Register (NIR) which will store basic personal information about the person in a secure manner;

iii) the ID card itself which could be used as a stand-alone card for proving a citizen's identity; and

iv) a verification service to confirm the identity of the cardholder or of the person whose biometric feature is registered on the NIR.

A number of technologies are required to ensure that the ID card operates in a robust way over many years of use. These include long-lasting material from which the card is made, a secure electronic data link between a card and the reader (eg by a contactless method such as in the new range of passports and in the Oyster card in use on the London tube), a Public Key Infrastructure which will ensure the integrity of the data stored in the card chip and finally, the application of biometric authentication to assure that the user has only registered once into the NIR, and that in subsequent use for high integrity transactions, the identity of the bearer of the card is indeed correctly confirmed.

Biometrics

Biometrics may be defined as automated methods of identifying people using a physical, physiological or behavioural characteristic. Some methods have been around for a long time (fingerprints have been a key tool for police forces for over a century), while others have been introduced very much more recently (for example, iris recognition was proposed just over 20 years ago).

All biometric systems start with the stored image of the biometric, which is normally recorded at an enrolment session. Subsequent verification of an individual's identity relies on comparing a presented biometric feature with this initially recorded biometric, typically using a proprietary pattern-matching algorithm that compares the characteristic elements in that biometric image with similar features stored at the enrolment. Because of the ever-changing ways in which people respond to the biometric terminal (for instance, they may smile or frown in a facial biometric system), this comparison will never be identical. Hence the need for a criterion for an acceptable degree of matching – the threshold value – which treads a fine line between security and usability. Allied to the selection of this criterion is a requirement to handle those exceptional cases where the individual hasn't quite been able to reach the threshold for acceptance.

The use to which biometrics are put affects the requirements put on the technology. For over a century, experts have compared the fingerprint marks left at the scene of crime with those obtained from previously arrested criminals. The collection of fingerprints on arrest involves a traditional ink and the rolled finger method with trained police officers guiding the fingers of the person to achieve the best impression. For the past 15 years or so, computer matching systems have been available to support the expert fingerprint examiners. However, a different approach is required for automated biometric systems. For example, optical imaging and even silicon chip sensors are used with the finger placed flat on a glass surface without the need to roll it from side to side. In many of these newer – biometric – systems the image is scanned to identify points where the individual fingerprint ridges either stop or branch into two separate ridges. The supplier of a biometric system will then use these 50-100 characteristic points (called minutiae) on each finger to create a template for that individual's fingerprint, and use proprietary algorithms to make a comparison between the set of points picked out when the person first enrolled and those identified at the time when their identity is being checked. A matching score can be derived using information from more than one finger and a threshold set based on the risk analysis. Procedures are needed for those people with missing fingers, where the surface ridges have been scarred, etc.

Different biometric technologies provide varying levels of matching performance and are suitable for different uses. Indeed, more than one biometric method can be used to decrease the number of people unable to provide a satisfactory verification; for instance, iris and face recognition can support the use of fingerprint technologies. Iris recognition relies on specialised algorithms working on the fine detail in the coloured part of the eye, in a way that keeps the information constant in spite of the changes in pupil size following changes in ambient light levels. One of the main approaches for automated face recognition uses a merging of a number of base facial images to approximate the image of the individual's face; the percentage of each of the base images is adjusted to optimise the accuracy of the resulting image. Another approach focuses on distinctive groupings of features relating to specific regions of the face.

The proper application of biometric technologies is at least as important as choosing the correct technology – or mix of technologies. For example, a high quality user interface and an optimised capture environment is necessary to put the person at ease to ensure that the best image is obtained. Security issues need to be addressed so that the biometric system will not accept plastic fingers with an impressed fingerprint or a photograph of a face. Of course, the needs of the elderly and disabled have to be taken into account as well.

Biometrics is an evolving field and we must be aware of what the future may hold for biometric technologies. Although the underlying biometric technologies are mature, commercial systems are constantly being improved with developments in increased usability, higher security against spoofed artefacts, and refining the underlying algorithms. For example, in facial recognition, three-dimensional imaging may reduce the impact of subjects not facing straight-on towards the camera. A key theme of much of this development is in fusing the results from more than one approach, whether it is just in taking two fingerprints or adding the scores from separate iris and fingerprint systems to give more confidence to the verification process.

Summary

Biometric authentication is at the heart of the proposed ID cards. Should the legislation be approved by Parliament, people in the UK will have a method of confirming their identity in a secure manner. The biometric technologies which are under consideration, using face, fingerprint and iris recognition, have been developed over several decades, although improvements are constantly being made. The key, however, will be to ensure that these are introduced in a standards-compliant system, which is secure, easily used by the vast majority of the population and in applications that provide clear benefits to the citizen, the foreign visitor and public and commercial organisations.