A Systemic Approach to Analysing the Implications of the Introduction of Biometric Passports

C. Hennell and V. Katos

School of Computing, University of Portsmouth, UK
email: {cheryl.hennell, vasilios.katos}@port.ac.uk

Abstract

This paper adopts a systemic approach to developing a holistic view in order to facilitate an understanding of the security and usability issues relating to the implementation and adoption of biometric passports. The main focus is to establish whether the proposed use of the biometric technologies should be used both for identification and authentication of the holder. Using the UK's National Identity Scheme (NIS) and National Identity Register (NIR) initiatives as a case study, we explore their proposals in the international context.

Keywords

Biometrics, Security, Usability, Rich Picture.

1. Introduction

It is a paradox that on a macro-scale we demand a freedom to live our lives and security from the governments that have the power to provide that security whilst on a micro-scale demanding that our personal civil liberties and privacy are sustained. Before 9/11 and enhanced since, the focus on terrorism and a need to protect national boundaries has gained momentum. Governments across the globe are passing laws that will support the introduction of identity cards (UK 2006) and the expedition of biometric passports (27 countries) in the name of protecting indigenous populations. The political and technical agenda sit outside the scope of this paper, however there are, as this paper will show, elements that are noteworthy of mention as they impact the human concerns over the use of biometric passport systems.

This paper addresses the question of whether biometric passports should be used as identification or authentication of the owner, and how this can be securely achieved. The paper is structured as follows: First we provide an overview of biometrics and the relationship with secure identification and authentication by mainly drawing on the work of UK Government bodies. We continue to discuss the relationship between security and usability of biometrics and the role of the user. Section 3 considers the UK Government proposals for implementing the information system to capture, store and process the biometric data. In Section 4, we discuss a selection of external

factors that might impact the success of the biometric passport system. Section 5 presents a systemic view of the discussions in the previous sections to provide a holistic image of the conflicts, concerns and issues related to the introduction of biometric passports. Based on the systemic representation, we conclude with a justification for our proposal to improve usability and security of biometric passports for identification and authentication, in the UK.

2. Biometrics and the Government

Biometrics can be defined as the use of anatomical, physiological or behaviour characteristics to recognise or verify the claimed identity of a person. It requires the collection, processing and storage of a person's physical characteristics (Coventry et al, 2003). Biometrics have a long history and are inextricably linked with forensic sciences: many of the emerging biometric areas are based on mature forensic disciplines.

The use of biometrics as identification and/or authentication is not however a new concept. There are some indications that biometrics were used by the ancient Egyptians to routinely record distinguishing marks. Pharaohs certified decrees with thumbprints and workers on pyramids were identified by biographical data and biometric data such as distinguishing features. In 14th century China, children's palm and footprints were recorded for identification purposes (Roberts, 2005)]. It is the IT security use of biometrics for identification and authentication in that is the emerging technology.

Traditional passports contain limited biographical data on the holder stored in two machine readable lines of OCR-B typeface. The standard format, data elements, field length and check digits comprise the first security measure that International Civil Aviation Organization (ICAO) invented for a passport. The photograph is used to confirm identity of the holder (McMunn, 2005). The traditional passports are not tamper proof and subject to forgery. In 1997, at the request of the ICAO, the New Technologies Working Group began a systematic study of biometrics and their potential to enhance identity confirmation. Adopting a scientific, quantitative scoring approach, the study chose to evaluate different biometrics against the unique requirements of travel document issuance and inspection processes. In their review of biometric technologies, the ICAO assessed their compatibility according to seven criteria, including:

- compatibility with enrolment requirements
- compatibility with MRTD renewal requirements
- compatibility with MRTD machine-assisted identity verification requirements
- redundancy
- global public perception
- storage requirements
- performance

- The results of the study (McMunn, 2005), based on their overall ability to meet the comprehensive set of requirements, were categorized into three groups:
- Group 1: Face achieves the highest compatibility rating (greater than 85%);
- Group 2: Finger(s) and eye(s) emerge with a second-level compatibility rating (near 65%); and
- Group 3: Signature, hand and voice emerge with a third-level compatibility rating (less than 50%).

These outcomes provide the basis for the development of the biometric passports currently being introduced by different governments as a mechanism to improve security at national borders. The validity of this adopted practice depends on the usability of the biometric passport and the human acceptance.

3. Security and Usability

The passport is conceptually a security token, something the holder *has*. As discussed, the *token* stores data on the holder and the holder does not need to *know* what the data are to be able to use the token to cross borders. This token is not secure. It is not tamper proof and it may be lost. However, for the holder, it is easy to use. The introduction of biometric passports should maintain the ease of use whilst increasing the security for the individual and the nation. There is a direct, if inverse, relationship between security and usability. In general the more stringent the security, the more it interferes with the user's experience causing a decrease in the usability of the system (Garzonis et al, 2004). There has been recognition that user behaviour plays a part in many security failures: it has become common to refer to users as 'the weakest link' (Sasse et al, 2001). User acceptance and behaviour have a direct impact on the successful adoption and implementation of biometric systems. Traditional passports are tokens that may be universally owned. Biometric passports require a different set of properties.

Biometric modalities can be classified by five desirable properties:

- Universal (available on all people)
- Invariant (features extracted are non-changing)
- High intra-class variability (features extracted are different from each user)
- Acceptable (characteristic is suitable for use by everyone)
- Extractable (a sensor can extract the features presented in a repeatable fashion) (Clarke, 1994; Wayman, 2000; Coventry et al, 2003; Kukula and Elliott, 2006).

To acquire a traditional passport requires the completion of documents and the presentation of a photograph authenticated by a *trusted* person. In the case of biometric passports, holders are required to enrol onto the system and for their biometric data to be captured and stored. In different business applications, a different biometric might be more appropriate than others. The iris being used quite

successfully where there is a high volume of people passing through a system, such as the expedited gate clearing at the airports (Courtney, 2005).

The introduction of biometric passports is being considered by governments across the world. The consensus of minimum data appears to be biographical in nature. Those biometric passports that have been considered appear to adopt the basic requirements of the ICAO, however, their implementation appears to be different. For example, Australia includes a PKI approach, whereas the Swedish passports use two chips (one for border control and one for accessing electronic services), unlike Singapore and Russia who use one chip.

However, some governments have decided to extend the scope in order to utilise the stored data for purposes other than purely border control. A particular case of interest is that of the UK government who appear to be using the introduction of the biometric passport to simultaneously develop the introduction of personal identity card.

3.1. The UK Government proposals

To further this discussion, we need to understand the UK Government proposals and intentions for the new biometric passport system. The UK Government has established a set of processes and procedures to set up a system to manage the biometric passports and identity card enrolments, data storage and data processing. This is known as the National Identity Scheme (NIS) (Home Office, 2006). In the plan they propose to deliver benefits in a number of key areas. These include securing national borders and tackling illegal immigration through effective identity management; reducing identity theft and identity fraud to fight crime and terrorism, and using the national identity scheme to protect vulnerable members of society, and to provide a shared data resource between government departments.

The Identity Cards Act 2006 outlines the main aims of the scheme as maintaining a secure and reliable record of facts about individuals in order to:

- prevent or detect crime;
- ensure national security;
- enforce immigration controls;
- secure the efficient and effective provision of public services; and
- enforce prohibitions on unauthorised working or employment (Garzonis et al, 2004).

The National Identity Scheme will be delivered by the Identity and Passport Service; the first Identity Cards are scheduled to be issued by 2009. The linking between the Identity Card and the issuing body provides an insight to the rationale for the collection and storage of both biographical data and biometric data for the biometric passports.

Biometric passports, including chips with the holder's facial biometric, were introduced in March 2006. These passports are in line with the standards set by the International Civil Aviation Organisation (ICAO) in May 2003, which nominated facial recognition as the primary biometric with iris and fingerprint as backup.

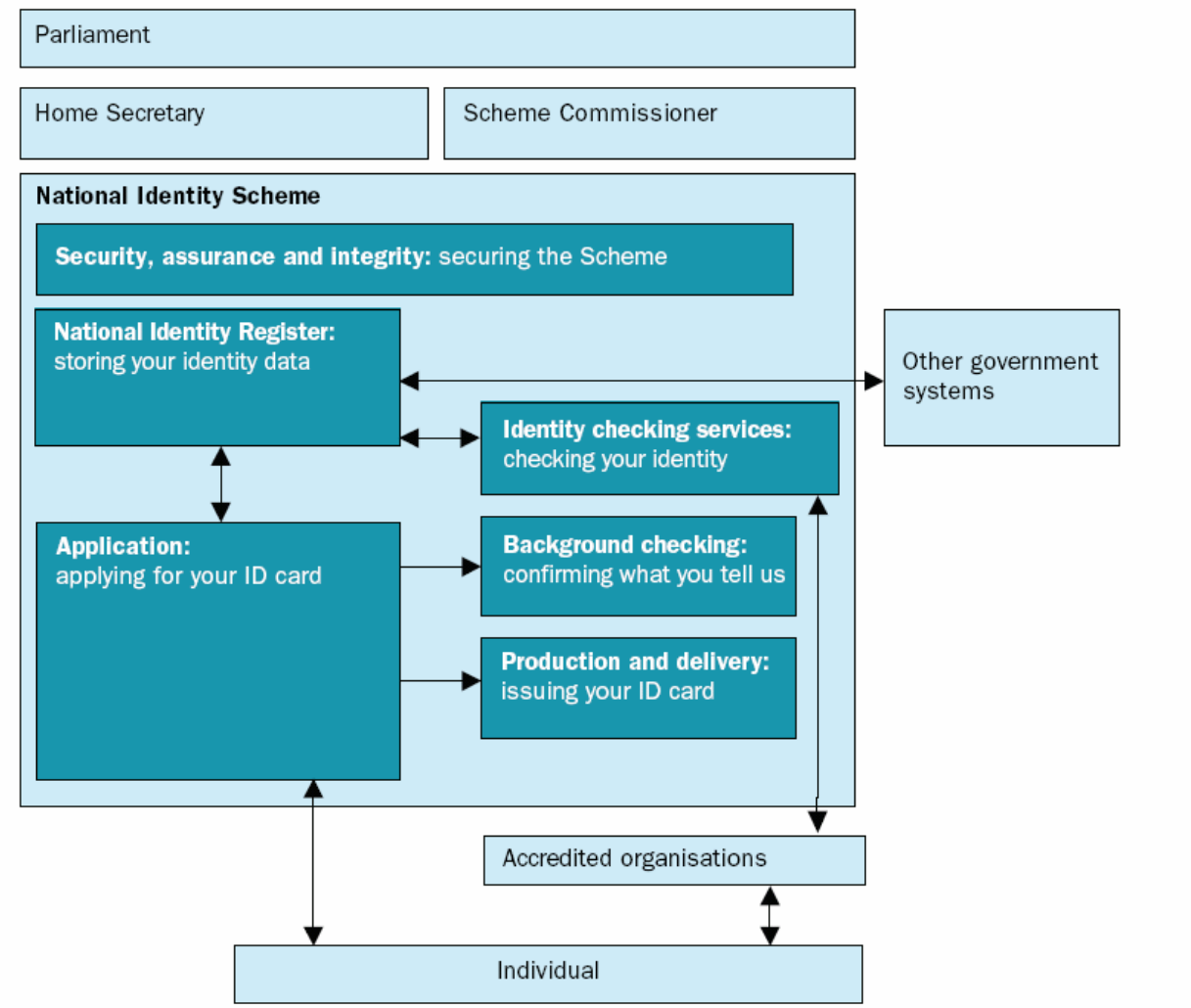

Figure 1: The National Identity Scheme model (source: Home Office, 2006)

The model clearly identifies the government's intentions to store biometric data alongside other personal and biographical data elements such as name, address and date of birth. The model also highlights the intention for the National Identity System to share this stored data with other government agencies. The government propose to store the data in a single logical database and on smart cards. Customised-of-the-shelf software modules will be used to process the data. The rationale for this approach is to simplify maintenance, to reduce risk and to highlight security violations as the data flows between the systems.

3.2. Issues

A number of studies have explored the technical perspectives relating to the various biometric devices, examining response times, Type I and Type II error sensitivity, data storage and retrieval times, and the cryptographic systems proposed to protect the data. Other studies have been conducted eliciting views from the general public through surveys to determine the acceptance levels by the British public of biometric passports. In the UK, the discussions relating to the biometric passport appear to be integrated with those of the introduction of the identity card. The latter has received a tide of negativity and overshadowed the introduction of the biometric passport. Whilst endorsing and supporting the need for an ID Card system, expert panel sessions and the LSE report have voiced concerns about the proposed system, and its ability to achieve its stated objectives within the current legislative and technology framework (Stevens, 2005). We need then to establish a secure system to identify and authenticate the holder of the passport to establish legal right of entry to the country. However, the authentication process is one of ensuring integrity, that the holder of the passport is who they claim to be.

Counterpoint to the usability claim of the biometric passport system as an effective and efficient security mechanism is the authentication of the holder. Herein lies the weak link to the perceived secure use of biometric passports. In order to gain a UK passport, the applicant needs to provide personal documents and data. This includes a birth certificate. Acquiring a birth certificate in not a difficult process and can now be undertaken on-line. Armed with a birth certificate and an application form, the applicant can assume the identity of any person. The biometric data will be captured, processed and stored on the biometric passport. As far as the system is concerned, the applicant's new identity is endorsed, with the biometric evidence as proof.

In the next section we consider a number of threat vectors related to the introduction of biometric passports.

3.3. Threat vectors

What does the biometric passport offer that conventional passports cannot? The passport demonstrates the owners' nationality and right to enter his/her own national boundaries. Whilst the traditional style passports have in the past been forgeable, it is intended that the introduction of biometrics should reduce this, strengthening the national border security.

It was mentioned earlier that in order for systems to succeed, the implementation must reduce 'the weakest link' – that of the human user. In this section we consider a number of external factors that initially appear to be unconnected. Collectively we perceive that these external factors create potential vulnerabilities which may be exposed to threat agents.

3.3.1 Identity Theft

The growing rate of identity theft, or at least the growth in the broadcasting of identity theft incidents have lead to public fear, uncertainty and mistrust. Many people have personally experienced financial loss and credit difficulties as a consequence of their identities being stolen. The public on the one hand are encouraged to protect their data both physical and soft, ensuring the use of strong passwords, firewalls and security software, and the secure destruction of identifying documentation such as household bills and credit card receipts. Ironically, on the other hand there is a perception that they are required to store all of their personal data and biometric data, the most sensitive personal data of all, on a digital chip in a single location, and of a questionable physical security. The difficulties faced in restoring one's financial status and credit rating, are challenging enough to provide sufficient convincing evidence of innocence. The challenges faced if ones complete biometric profile is stolen could be insurmountable.

3.3.2. Privacy and Human Rights

The UK Government's proposals to store unprotected biographical and biometric data on the passport chip may have serious personal consequences. Privacy International (2004) have stated that "The ICAO is aware, however, that there are contentious legal issues involved with the infrastructure for these passports, including the collisions between the goals of centralizing citizens' biometrics and protecting privacy laws, and with 'cultural practices'. Not only does this involve a central data store of fingerprints and photos (and face scans) that can be scanned against other databases for other purposes, but this sensitive information may be transferred to other countries when verification is required at border controls. The ICAO foresees that this information may be retained by these other countries. In essence, this may turn into a global distributed database of personal information.

3.3.3. Departures and Arrivals Airport Security

Since the events of 9/11, there has been a noticeable increase, decline and then increase (following 7/7 terrorist attacks in London) of security measures at UK airports. Baggage security, personal security checks and searches heightened slowing down the movement of passengers. However, automated biometric passport controls have been implemented which enable passengers to conduct their own passage through border controls. The microchip embedded in the passport can be read by a special chip reader, while digital signatures verify the data's authenticity, or reveal if the data has been tampered with (O'Brien, 2006).

In Singapore, the Automatic Border Control (ABC) System replaces the manual immigration clearance process with a more efficient and secure system, thereby eliminating human error while heightening security significantly. The automated operation uses a hybrid biometric authentication – NEC Facial Recognition and NEC Finger Identification - to reduce a previously 15-minute process of immigration clearance to mere seconds with the highest accuracy achievable today. The ABC

System also offers immigration authorities the added advantage of re-deploying limited resources to other important functions (NEC, 2005)]

For those airports without automated passport controls, the performance of the technical platforms will control the footfall through the arrivals and departures gates. In addition to the fully automated ticketing processes now offered by some airlines, the role of the human at the border controls appears fragile and diminishing. The reliance on technology for human identification and authentication is extending its reach.

3.3.4 Lost passports

As Reid states "With the old passport, we knew where we stood. If you lost it you knew you had lost it, but with the new, machine readable passports the story is very different. When you take a digital photo the image is, in effect, a code, which means that however many prints you make they are all exactly the same" (Reid, 2006). The loss becomes virtual and often undetected by the holder.

3.3.5 False Accept and False Reject

The choice of technology and the performance levels pre-determined will impact the usability and user satisfaction of the system. The level of sensitivity, the crossover error rate of such systems will govern the number of illegal entrants accepted and the number of legal entrants rejected. Either situation would be unacceptable to the individual concerned or to the wider public in the event of an illegal being granted entry contradicting all government promises.

4. Analysis of the problem – A Systemic Perspective

As for any proposed system, adopting a reductionist view analysing the elements in isolation creates a potential conflict in operations and diminishes potential system success. The systemic approach adopted here provides a holistic view of the issues previously discussed, collected and collated in a rich picture. Rich pictures offer a benefit over process models, capturing human thoughts, views, feelings, and drawing out the support and conflict relationships between the various elements within the system. The rich picture in Figure 2 was developed using data drawn from a wide range of documents including news reports, journal articles, white papers, discussion boards, security briefing documents and academic papers. These rich sources provide multiple perspectives from diverse backgrounds.

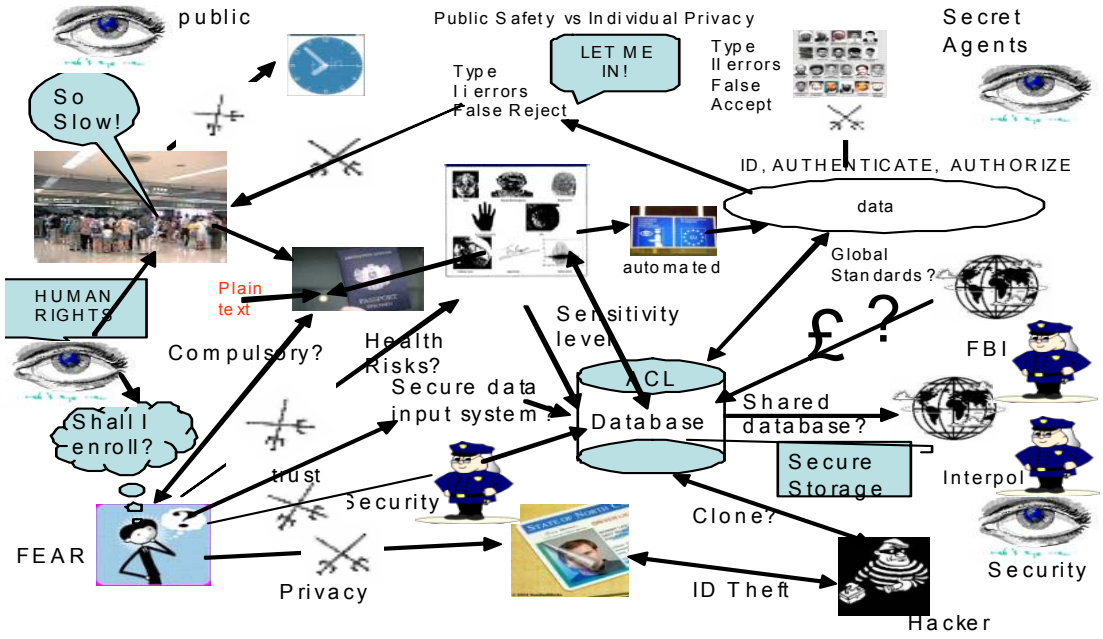

Figure 2: The rich picture

A number of issues become apparent when adopting a holistic view of the problem, as captured in the rich picture in Figure 3. As mentioned earlier in this paper, the main focus is to investigate whether biometric passports could be used for both identification and authentication purposes.

An obvious flaw in the whole approach is the assumption of the consideration of Type I and Type II errors in the security process. The calculation of the false rejection and false acceptance rate assumes that the biometric storage facility has not been tampered with. Consequently, the assumption of the adversary is limited to a person who is attempting or hoping to gain access as part of the false acceptance state of the system. Although the granularity of the analysis of the feasibility of a biometric system is increased with the introduction of additional metrics - such as the false match and non-match rates and the failure to acquire rate - a malicious adversary introducing protocol failures (say through spoofing) is not extensively studied in a biometric passport control system. In other words, the false acceptance and false rejection rates would have no significant meaning (other than user acceptance metrics) in the case of a biometric passport border access control system. This is because calculation of these rates needs to be performed in a "sterile" environment, where there is *a priori* knowledge on the validity and integrity of the authenticated subjects and the data they are holding. A malicious adversary by tampering successfully the biometric data storage would in effect invalidate the false acceptance rate, as it will not be possible to objectively calculate this metric. In addition, the false rejection rate could still be valid, but any failure to successfully authenticate would be treated as the system sensitivity rather than a security breach issue. Consequently, in order to overcome the spoliation of the false accept rate, authentication would need to be performed by other means, whereas the biometric data would be limited to supporting only identification.

The assumption of the malicious adversary was addressed at the Black hat Conference in Las Vegas, 2006. More specifically, Grunwald (2006) demonstrated that it is trivial to copy the biometric certificate from an open e-passport into a standard ISO 14443 smartcard using a standard contact-less card interface and a simple file transfer tool. In particular, Grunewald did not change the data held on the copied chip, which binds biometric data (e.g., photo) to identity data (e.g., name and date of birth), without invalidating its cryptographic signature, which means at present the use of this technique does not allow reprogramming of fake biometric data to match a different user. Grunwald also did *not* clone the Active Authentication functionality, an optional feature of the ICAO e-passport standard that some countries implement such that the embedded microprocessor is not only a floppy-disk-like data carrier for a biometric certificate, but also a tamper-resistant authentication token that can participate in a public-key-cryptography based challenge-response protocol. Nevertheless, Grunewald created international media headlines with his claim that such copying of the biometric certificate constitutes the creation of a "false passport" using equipment costing around USD$200.

Furthermore, a group of German privacy hackers have come up with a portable device that can wipe a passive RFID-Tag permanently. In this case the adversary would target the availability of the data, mounting a large scale denial of service attack, and this would have an impact to false non-match rate (Farrell, 2006).

The concerns regarding the implementation of biometric passports transcend national boundaries. "Nearly every country issuing this passport has a few security experts who are yelling at the top of their lungs and trying to shout out: 'This is not secure. …. There are lots of technical flaws in it and there are things that have just been forgotten, so it is basically not doing what it is supposed to do. It is supposed to get a higher security level. It is not." (Reid, 2006).

Whilst endorsing the need for biometric systems, the evaluation panels and the LSE report have voiced concerns about the proposed system, and its ability to achieve its stated objectives within the current legislative and technology framework (Stevens, 2005).

5. Conclusions

The implementation of biometric passports is unstoppable. Introduced in the wake of terrorist activity by governments on a global basis, individuals must accept them. The current approach to biometric passports is to strengthen its tamper resistance, increasing the effort and resources required in order to forge them. As discussed, this is not the case, since methods to crack the electronic data have been published. Thus it would appear that biometric passports cannot be used to authenticate the holder. As a direct consequence, the expectation that biometric passports would help in automating the border controls processes cannot be met, as identification and authentication would still require human intervention.

The usability of a biometric passport system requires the acceptance of all users that the system will protect their persona and provide an acceptable level of usability. To quell the anguish of future passport holders, the government need to instil confidence and the system must be fit for purpose. Instilling confidence in passport holders may be achieved through an appropriate education and communication mechanism. However, without the evidence of trust, the holders will adopt the biometric passport system reluctantly, not necessarily by choice but by force. It will take another nine years before the biometric passport system can be fully implemented.

From our analysis of the discussion, we conclude that biometric passports should contain sufficient data to enforce national border controls to establish the identity of the holder. To automate this activity and provide authentication, more secure approaches are needed. We propose a further study into the adoption of a number of potential cryptographic techniques such as one way hashes, one-way keyed hashes, Manipulation Detection Codes, to provide a secure, tamper proof environment to store the data.

References

Clarke, R. (1994). Human identification in information systems: Management challenges and public policy issues. Information Technology & People, 7(4), 6-37.

Courtney, K. (2005), Select Committee on Science and Technology, sixth Report, www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/103205.htm

Coventry, L., De Angeli, A., and Johnson, G. (2003). "Usability and biometric verification at the ATM interface," Conference on Human Factors in Computing Systems Ft. Lauderdale, Florida

Farrell, N. (2006), German privacy hackers develop RFID zapper: Destroys passive RFID tags at a glance, The Enquirer, http://www.theinquirer.net/default.aspx?article=28737

Garzonis, S., O'Neill, E., Kostakos, V., Kaenampornpan, M. and Warr, A. (2004), A Novel Approach for Identification and Authentication of Users in a Pervasive Environment, proceedings of the 2nd UK-UbiNet Workshop, HCI Group, University of Bath

Grunwald, L. (2006), New Attack to RFID systems and their Middleware and Backends, Black Hat conference, Las Vegas, August

Home Office (2006) Strategic Action Plan for the National Identity Scheme: Safeguarding your identity
http://www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/103205.htm#a4

Kukula, E. and Elliott, S. (2006) Implementing Ergonomic Principles in a Biometric System: A Look at the Human Biometric Sensor Interaction, www.biotown.purdue.edu/research/ergonomics.asp

McMunn, M. (2005) Machine Readable Travel Documents with Biometric Enhancement: the ICAO Standard, Optimizing Security and Efficiency Through Enhanced ID Technology ICAO MRTD Report, Inaugural Issue, Volume 1, No 1 http://mrtd.icao.int//downloads/publications/MRTD_Report/MRTD_Rpt_V1N1_2006.pdf

NEC (2005) NEC unveils its 3D Facial Recognition System for first time in Asia (outside Japan) at Global Security Asia 05, www.nec.com.sg/bccs/News/2005/050328.htm

O'Brien, C. (2006) E-passport launched in Ireland: In the nick of time, ElectricNews.Net

Reid, D. (2006) British ePassport, news.bbc.co.uk/2/hi/programmes/click_online/6182207.stm

Roberts, C. (2005) Biometrics, http://www.ccip.govt.nz/ccip-publications/ccip-reports/Biometrics.pdf

Sasse, M. A., Brostoff, S. and Weirich, D. (2001), Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. BT Technology Journal, - Springer

Stevens, T. (2005) The Identity Project: The Identity Cards Bill, and its potential impact on UK academic institutions, Director, Enterprise Privacy Group http://www.jisclegal.ac.uk/events/privacy05/Presentations/Stevens_paper_privacy.doc

Wayman, J. (2000). Fundamentals of Biometric Authentication Technologies. In J. Wayman (Ed.), National Biometric Test Center Collected Works 1997-2000 (1.2 ed., pp. 1-20). San Jose.