[*Note. The original of this document was submitted to the Home Affairs Committee of the UK Parliament (House of Commons). For this version, dated 16th January 2004, there have been 3 minor amendments to improve clarity plus some typographical corrections.*]

Comment on Government Proposals for Identity Card Scheme

5th January 2004 (Annex to Letter: S/03017/comment_NIdS/L031219a.rtf)

Nigel Sedgwick

Cambridge Algorithmica Limited, 9 Oakdene, Beaconsfield, Buckinghamshire HP9 2BZ
tel: 01494-678989; fax: 01494-678990; email: ncs@camalg.co.uk

Introduction

1. I am responding to your request dated 19th November 2003. My comments come principally through my technical expertise in the field of biometrics, and also through some additional expertise in the fields of computer security and communications security.

2. The covering letter and this annex are being sent by email. A signed top copy of the letter, the annex and copies of references [9] and [10] will also be posted.

Information on the Author's Technical Background

3. My technical experience spans 29 years since graduating from Imperial College in Physics (BSc, ARCS in 1974); I also have a degree in Computer Science (MTech, Brunel 1980). I am a member of: the Institution of Electrical Engineers, the British Computer Society and the Institute of Acoustics. I work on pattern matching and digital signal processing, through my personal trading company (Cambridge Algorithmica Limited), undertaking technical consultancy and contract research and development. This work is principally in the fields of biometrics, automatic speech recognition and data modems. Much of my work has been for the UK Government, and is of a highly technical nature. In the field of biometrics, I personally have worked on speaker verification/identification, dynamic (hand-written) signature verification and multi-modal biometric combination.

4. In the middle of last year, I was appointed to the British Standards Institute Committee IST/44 on Biometric Standards, in the capacity of Principal UK Expert.

Overview of the Governmental Context

5. The Government deserves credit for its decision to tackle the large and growing problem of identity-related fraud. In particular, the provision of a National Identity Scheme (NIdS) is an excellent approach. Furthermore, the Government's intention to make available the NIdS for non-governmental applications (particularly business/commercial use to reduce financial fraud) will be a generally useful service to the public.

6. However, as has been pointed out by many critics of the Government's proposals, there are political, legal and technological difficulties. My expert contribution is primarily on the technological issues.

7. The proposed NIdS[1] has some serious technical shortcomings. There are technical solutions to remove or mitigate most of these. However, this is at increased cost; there is also contingent need for practical procedures that are more onerous to operate. I am optimistic that careful consideration now, within the wider political and social context, will allow implementation of a viable NIdS that is effective and beneficial to society as a whole.

Principal Points on Application of Biometric and other Technology

8. **There should be separate biometrics for Detection of Multiple Applications (DMA) and for Point of Use (PoU) Authentication**. The technical requirements for these are substantially different; they are better handled by biometric systems designed primarily for these different purposes. Potential cost reductions from exploiting commonality should be viewed as secondary; otherwise performance and practicality will be compromised.

[1] As far as one can judge from the descriptions in the public domain (see references [1] to [6]).

9. **Biometric templates should be held centrally, not on ID Cards**. Storing *templates* or *reference patterns*[2] on ID Cards makes the whole system more vulnerable to several forms of attack. These risks can be reduced or avoided, probably at lower overall cost, by storing templates on a central database and forwarding biometric samples, taken at the PoU, to a central computer for authentication.

10. **Multi-modal biometrics are necessary for adequate overall performance**. For Detection of Multiple Applications (DMA), no known single biometric device is adequate. Use of two or more different and well-chosen biometric devices, together with multi-modal combination, should provide sufficient performance. Multi-modal biometrics also offer improved *universality*[3] and make sophisticated attack more difficult. These latter benefits are also important for PoU authentication.

11. **Smart cards are vulnerable to forgery; excessive reliance should not be placed on them**. Despite the best efforts of card manufacturers, it will eventually be possible to access the data content and reverse engineer any smart card (see, for example, [7] and [8]); forged cards can then be produced. Though this will be at a price, it will not be beyond the means of organised crime. Cryptographic techniques do give further protection; however, practical constraints make on-card encrypted information more vulnerable than encrypted information transmitted over communications networks.

12. **PoU authentication is available without compulsory carrying of ID Cards**. A registered person's identity can be verified, by biometric check, even if they do not have their card with them. Their full name and address will, almost invariably, be adequate for a claimed identity; verification of one or more biometric samples against their centrally held template(s) will confirm their identity[4]. For less secure use, without a biometric device being available, obviously a quick visual check can be made against an ID Card displaying a photograph (and other details such as sex and age).

13. **Registration stations on non-government sites may be too vulnerable**. These sites and their NIdS staff are likely targets for identity fraud attacks. It is questionable whether sufficient security can be provided at registration stations located on non-government sites.

14. **Deterrence of fraudsters requires timely DMA and the threat of immediate arrest**. Biometric detection, of applications in multiple identities, is not foolproof. High risk of detection and severe penalties, together, form the deterrent. Given the likelihood of being unable to trace fraudsters after they leave the registration site, DMA checks need to be made before then; this requires fast matching on NIdS central computers. Also, immediate arrest and detention must be practical.

Further Information on Detection of Multiple Applications (DMA)

15. The Government's paper [3] gives some useful analysis. As they point out, checking against 50 million previously registered persons needs a very low False Match Rate (FMR); otherwise, there would be an unmanageably high number of applications requiring additional manual checks. However, it seems unlikely that the Government's estimated False Non-Match Rate (FNMR) of 5% to 10% of fraudulent applications would provide sufficient deterrence. This is especially if they propose that applications would not be subjected to biometric check until after the applicant has left the site.

16. Use of multi-modal biometrics (eg a combination of iris scan, multiple fingerprints and perhaps other physical biometrics[5]) would give both low FMR and low FNMR, thus providing adequate deterrence against multiple applications.

[2] Templates or reference patterns are (or are created from) the biometric sample(s) given during enrolment.

[3] Universality is a highly desirable feature of a biometric device: that all persons can provide samples and are willing to. Unfortunately however, there is some lack of universality of biometrics; there are genetic traits that make iris recognition less effective; fingerprints are degraded in some occupations; etc.

[4] Possession of the ID Card provides additional protection. However, verification using multi-modal biometrics forms an adequate substitute, up to any chosen level of security.

[5] It should be noted that multi-modal combination can benefit from inclusion of biometrics that have poor performance, relative to the other biometrics used.

17. In addition, universality is improved. Those unable (or unwilling) to offer each single type of biometric should be able to provide say 2 out of 3. Finally, circumvention by self-mutilation is likely to be much less successful against multi-modal biometric DMA.

18. To support DMA before the applicant leaves the registration site, matches against all previously registered persons need to be done within say 20 minutes (during which time other aspects of registration could be undertaken). For this, towards the end of the initial registration of the bulk of the population (at some 2,000 registration sites and assuming 3 individual biometrics), the central NIdS computer would need to be able to match biometric samples at the rate of about 250 million per second. This is high, but not beyond practicality. Note that the overall throughput is only about 4.2 times higher than that required for later matching; this is assuming that matching 24 hours per day 7 days per week keeps up with applications arriving every 20 minutes, from each registration site during a 40 hour working week.

Further Information on Point of Use (PoU) Authentication

19. It is assumed in the Government's current plan that PoU biometric templates or reference patterns will be stored on the ID Card, which will be a smart card with sufficient digital memory for this. The PoU terminal/computer will capture the biometric sample and match it against the decrypted template obtained from the ID Card.

20. My recommended alternative is for templates to be stored only on the central NIdS computer; then one or more biometric samples captured at the PoU are transmitted[6] to the central NIdS computer for matching. This approach has several technical advantages.

21. **Attack against the biometric template is more difficult**. If stored on the ID Card, the decrypted template is vulnerable following card theft. This is because PoU computers must be able to access it for matching (and such terminals are vulnerable to reverse engineering). One simple attack is similar to exhaustive search: find which person (in your organised crime syndicate) has the best match against the template on each stolen card; then that person uses the card (pre-block) to perpetrate fraud.

22. **Cost of smart card**. Without the need to store template data, a lower cost smart card could be used.

23. **Multi-modal biometrics**. With template storage on the card, this option becomes more expensive. Storage of multiple templates on the central NIdS computer is much less expensive; this is required anyway, though not necessarily with fast access.

24. **Encryption vulnerabilities**. It is assumed that data stored on the ID Card would be encrypted, using a trapdoor encryption algorithm[7]. The same key (or a modest number through some key compartmentation scheme) is used for every card; breaking the key creates a widespread vulnerability that is very expensive to overcome. For an encrypted communications system, each link can use a different key and keys can be changed frequently; thus, if there is compromise of a crypto key, damage is much more limited. The cryptographic strength is less, for trapdoor encryption algorithms.

25. **Substitution of biometric template**. If the encryption key for the trapdoor encryption algorithm is compromised, fraudsters would be able to create (without limit) fake ID Cards containing their own biometric templates.

Further Information on Choice of Biometric Devices

26. The Government's choice of biometrics for DMA, of iris or multiple fingerprints, is good. However, using just one is unlikely to give (simultaneously) adequate FMR and FNMR. Both should be used together for DMA. In addition, any physical biometric selected for PoU could also be used to improve DMA, always or in cases where matching of the primary DMA biometrics was inconclusive.

[6] Transmission of some information is necessary where validation of the card is done (as it surely must be to protect against fake and blocked cards). Presumably this will be done over the Internet, or a private government network that uses the same (TCP/IP) protocols. With care, the total amount of data would still be sent in a single packet, with negligible extra communications load and transmission delay.

[7] Otherwise, biometric templates could be substituted easily.

27. Face recognition is less obviously a good choice. There are alternative physical biometrics, such as hand geometry, ear lobe geometry and vein patterns in the hand. Current levels of performance for face are variable, and not obviously better than the competition. In addition, there are behavioural aspects to face, including choice of hair style and use of makeup; ageing is also more problematic than with other biometrics. Face is not suitable as a primary biometric for DMA, and so should only be part of the NIdS if chosen for the PoU. The choice of face by The International Civil Aviation Organisation (ICAO) for Machine-Readable Travel Documents (MRTD) should itself be reconsidered. Whilst compatibility with ICAO MRTDs is desirable, it is not the only factor. This is especially considering the extra flexibility given by multi-modal biometrics. For the UK NIdS and at this early stage, it seems premature to choose face to the exclusion of all other PoU biometrics.

28. At the PoU, one or two fingerprints is also a good choice. If fingerprint templates were those captured for DMA, this would reduce enrolment time at registration stations.

29. Behavioural biometrics should be acceptable for PoU, in some cases, as a matter of convenience. In particular, for credit/debit card transactions (surely a major application), hand-written signature has known advantages (see [9] and [10]) including widespread public acceptability, reasonable performance and (in one form: acoustic emission) a very low cost sensor.

Comment in 1995

30. I made extensive comments ([9], copy in post) on the green paper issued by the previous Conservative Government. A non-technical presentation was made to the Association for Biometrics, based on those comments ([10], with viewfoils also in the post).

31. Although the technology has advanced, the majority of these comments still apply. One particular change is the addition of iris recognition to the available physical biometrics that are well tried and acceptable to the public. This is a key point, given the excellent performance of iris recognition.

32. Public acceptability of biometrics, and of the need for NIdS, has also improved. Whether compulsory registration with an NIdS is acceptable to the general public remains an open question in my mind. Certainly, I would not be happy without significant legal safeguards, against government misuse and over-zealous public officials.

References

[1] ***Identity Cards: The Next Steps***, Cm 6020, November 2003.

[2] ***Identity Cards: A Summary of Findings from the Consultation Exercise on Entitlement Cards and Identity Fraud***, Cm 6019, November 2003.

[3] ***Feasibility Study on the Use of Biometrics in an Entitlement Schem***e, version 3, February 2003, National Physical Laboratory.

[4] ***Answers to Top Questions on Identity Cards***, Home Office Website, 11 November 2003.

[5] ***Identity Fraud: A Study***, Cabinet Office, July, 2002.

[6] ***Uncorrected Transcript of Oral Evidence taken before the Home Affairs Committee***, The United Kingdom Parliament, 11 December 2003.

[7] ***On a New Way to Read Data from Memory***, David Samyde, Sergei Skorobogatov, Ross Anderson and Jean-Jacques Quisquater, Workshop on Cryptographic Hardware and Embedded Systems, August 2002 (CHES 2002).

[8] ***Camera Flash Opens Up Smart Cards***, Will Knight, New Scientist, 13 May 2002.

[9] ***Comment on Green Paper on Identity Cards***, letter by Nigel Sedgwick (Cambridge Algorithmica Limited), to the Government's Identity Card Green Paper Unit, 30 September 1995.

[10] ***Some Issues for a National Identity Card – Biometric Roles***, presentation by Nigel Sedgwick (Cambridge Algorithmica Limited), to the Association for Biometrics, 22 November 1995.