UK COMPUTING RESEARCH COMMITTEE

Comments by the UKCRC on "An assessment of the technologies needed for a National Identity Cards Scheme"

1. This document comments on the discussion of the technological feasibility of ID cards set out in the above briefing paper written by the ID Technology Advisory Group. For brevity, we refer to this document as "ID-Tech-Doc" in the discussion below. We refer to the national identity management system as UK-NIR.
2. This paper is presented by the UKCRC – an independent body of distinguished computer science researchers drawn from industry and academia. The UKCRC has no involvement with any suppliers of ID card technologies.
3. A significant concern of the UKCRC is that the document, as presented, cannot be objective as the authors have an interest in the supply of ID card technologies.
4. The ID-Tech-Doc is unequivocal in its views that "a national identity management scheme is technically feasible". It is our view that this conclusion is premature. The goals, scope and requirements of the national identity management system have not yet been established and definitive judgements on the feasibility of this system in the UK requires a detailed analysis of the system goals and requirements and cannot be made until this information is available.
5. In several places in ID-Tech-Doc, reference is made to ID card systems that are in use elsewhere in the world. We cannot comment on the success or otherwise of such systems but make the point that it is unclear if they are comparable in their scope, goals or scale with the proposed UK-NIR. Without details of both the UK-NIR and these other systems, valid comparisons simply cannot be made.
6. The ID-Tech-Doc identifies a number of operational success factors for the UK-NIR namely speed, security, scalability and stability. We agree that these factors are important. However, factors such as availability (is the system able to deliver services when requested to do so), reliability (will the delivered services be correct) and accuracy (will the data maintained by the system be accurate) are equally important and are not considered in the ID-Tech-Doc. Issues of accuracy are particularly problematic – what technical and organisational mechanisms will be put in place so that citizens can check that their information is correctly recorded and maintained by the system? If errors are discovered, how will a citizen ensure that these errors have been corrected?
7. When considering operational issues, it must be borne in mind that the UK-NIR is not simply a technical system involving a very large database of biometrics. Rather, it is a complex socio-technical system with dynamic interactions between people, organisations and technology. Such systems evolve to cope with changing circumstances and, in general, this contributes to more effective operation. However, it does mean that, whatever the quality of the hardware and software used, there remains the possibility that failures will occur because of human and social issues. For example, mistakes made during a relatively simple upgrade procedure recently resulted in a widespread loss of service from the Department of Work and Pensions.
8. *Scalability*. Comparisons are drawn here between the UK-NIR and other large-scale database systems. Without doubt, it is technically possible to store and manage large volumes of data. However, without detailed requirements for the UK-NIR, it is impossible to know if the comparisons made here are valid.

9. *Speed*. It is claimed that the US fingerprint database checks take approximately 15-20 seconds. However, it is not clear if this is an average or worst case figure? Nor is it clear if this per fingerprint or for a complete person check? Speed of response is dependent on the number of demands made in some given period of time. Without information on where the system will be deployed and the extent of its use, it is impossible to come to conclusions about these demands and whether the responsiveness of the system will be acceptable.
10. *Stability and resilience*. It is claimed in the ID-Tech-Doc that using “full failure protection and remote standby using real-time synchronization” can mean that, “zero downtime” can be achieved. There are no technologies currently available that can guarantee zero downtime. Further, failures that lead to system downtime are not always failures of technology. Human error is a significant cause of system downtime and simple replication cannot necessarily compensate for such errors. It is practically impossible to design systems that are resilient to all possible human errors.
11. *Security*. It is claimed that design and implementation options can 'prevent failure and attacks of all forms'. This is an unjustifiable claim. Of course, appropriate technologies can deter attackers by increasing the costs of attacks and reducing the probability that these attacks will succeed. However, security can NEVER be guaranteed. The ID-Tech-Doc makes a comparison with the banking industry which, undoubtedly, has spent large sums improving system security. Banks do, however, still suffer from security failures; to quote the Central Sponsor for Information Assurance (CSIA) (their web page on risks): “In the National Hi-Tech Crime Unit's 2003 survey, 83% of businesses stated that they had experienced some form of hi-tech crime. Of the 44 financial institutions surveyed, three companies had experienced a fraud worth more than £60 million.” It also seems likely that the losses are underreported (for reasons of customer confidence in the systems.)

    As a body of computer scientists, we cannot comment on processes for secure collection or delivery of sensitive documents. However, we note that identity theft through documents that are misdelivered is reported to be an increasing problem. It may therefore be unwise to be complacent about existing processes. The theft of many hundreds of cheque-books by a postman, reported recently, underlines the difficulty of secure delivery.
12. *Enrolment*. The estimates of the time required for enrolment here were made without the use of technology. The technological assumptions made are not discussed here. It is our view that credible estimates cannot be made without some knowledge of the likely performance (both in terms of responsiveness and accuracy) of the technology.
13. *Verification*. The key issue here, which is not discussed, is accuracy. How reliable and accurate is the equipment that captures the biometrics and how accurate is the stored information in the database? It is not clear how failures due to inaccuracy will be handled.
14. *Biometrics*. A key issue identified here is to ensure that an applicant is not already enrolled with the system under a different identity. It is suggested that this will involve comparison with all biometrics already held in the database. This involves comparison with a very large number of records and no information is provided here on the assumptions made about the time required for this. Given that it is suggested that the retrieval time for a single record is 10-15 seconds, we are concerned that the time required for such checks could be excessive (records do not have to be checked one after the other, but there is a limit to how much “speed up” can be achieved by checking records in parallel, at a reasonable cost).

    We agree that the specific biometrics identified are feasible candidates for inclusion in a UK-NIR. Again, however, more details of the purpose and scope of the UK-NIR are required before final conclusions can be drawn about the specific biometrics used.

15. *Smart cards*. Our concerns here are not on the smart card technologies themselves but on the statements made here under 'System security". It is stated that "The UK Financial community runs large IT systems which, by their nature, are subject to attack and repel (sic) them day by day using tried and tested methods and products from the IT security industry". We refer to the point made previously that, in spite of the best efforts of financial institutions, serious security problems have arisen in their financial systems. The information supplied by the CSIA does not seem to us to show that the banks successfully "repel" attacks. We also refer to point 7 above – security is a socio-technical not simply a technical issue.
16. *Conclusion*. We have already referred to our concerns about the conclusion that such a system is technically feasible. We are also concerned by the statement that "technology will not be the limiting factor". It is certainly true that technology will be ***a*** limiting factor – the extent of these limits will depend on the overall goals of the UK-NIR.
17. The ID-Tech-Doc made no reference to issues of procurement and the processes of procurement, specification, design, development and testing of the UK-NIR. We would point out that, historically, many problems have arisen in the procurement and deployment of large public sector systems in the UK (e.g. Child Benefits System, Passport System, etc.). It should not be assumed that all such problems have been resolved or, indeed, are resolvable.
18. The problems of complex systems engineering are not simply technical problems – there are inherent problems of complexity and changing requirements in large systems that mean that initial planning assumptions rapidly become out-of-date. Given the enormous complexity of the UK-NIR, it is inevitable that changes will arise. Significant contingency both in terms of budget and schedule must be allowed for to cope with changes in any such system development.
19. Notwithstanding these inherent problems, we believe that it is essential to use best practice in software and systems engineering in the development of such systems in order to minimize the technical problems of systems development. Particular attention must be paid to achieving a precise specification of the requirements for such a system and in carrying out extensive simulations and prototyping before commitment to a particular systems proposal is made.
20. The UK-NIR will necessarily have a completely different status from existing systems on which many of the ID-Tech-Doc claims are based. It will have a fundamental formal and operational status as the basis of citizenship for every individual citizen in the UK. For this reason alone it requires an altogether higher standard of design, specification, implementation, and operation than ordinary database systems, however large, complex and important they are. In the UKCRC's view, the ID-Tech-Doc does not recognise this. So the claims the ID-Tech-Doc makes that the UK-NIR can be successfully established on the basis of current supplier experience are open to question.

Prof. Ian Sommerville, Lancaster University, for the UKCRC

9th December 2005.