UK COMPUTING RESEARCH COMMITTEE

Draft Identity Cards Bill and Consultation Paper

UKCRC comments to the Home Office

The UK Computing Research Committee (UKCRC), an Expert Panel of the British Computer Society, the Institution of Electrical Engineers and the Council of Professors and Heads of Computing, was formed in November 2000 as a policy committee for computing research in the UK. Its members are leading computing researchers from UK academia and industry.

UKCRC has the expertise to address the first two questions identified by the committee:

- the practical issues involved in the ID database and biometric identifiers;
- the security and integrity of the proposed system.

This response to the consultation has been written specifically for the Committee.

Although we do not wish to comment ourselves on the social, legal and operational issues of ID cards, we strongly recommend that the committee obtains a copy of the (slim) report IDs—Not That Easy produced by the Computer Science and Telecommunications Board of the US National Academy of Sciences in 2002, whose dispassionate analysis of the key issues appears to us to be very helpful in considering these wider issues. The report may be found on the Internet at http://www7.nationalacademies.org/cstb/pub_nationwideidentity.html. A copy of the Executive Summary of this report is appended. Bruce Schneier, a leading US security expert, has published a well informed essay on some issues relating to ID cards. This may be found at http://www.schneier.com/crypto-gram-0112.html#1.

1 The Practical Issues Involved In The ID Database And Biometric Identifiers

The Home Office plans to introduce biometric identity cards (passports, driving licenses) to counter "growing threats to security and prosperity of British Citizens from illegal migration and working, organised crime and terrorism, identity theft and fraud and fraudulent access to public services" (http://www.homeoffice.gov.uk/comrace/identitycards/index.html).

This statement does not amount to a statement of requirements or a specification that would be adequate to begin designing a technical solution. The answers to the following questions are needed to ensure that any technical requirements that may be drawn up for the system actually meet the real-world requirements. If they do not, it is inevitable that the technical requirements will change, leading to delays, cost escalation, and loss of control over project risks. We are advised that that a current study of problems of large scale projects by the Royal Academy of Engineering will report that poor project definition is one of the major contributors to project failure. The Academy will also observe that there is a greater tendency for poor project definition in the public sector, where systems are intended to meet political ends, and the practicalities often have not been thought through.

1.1 Top-level objectives

- Has any independent study been undertaken to establish that the threats identified by the Home Office as requiring the introduction of ID cards are significantly lower in countries that already have ID cards?
- If so, what specific lessons can be learnt from existing national ID card systems?
- If not, what evidence exists that the proposed UK system would have the desired benefits, and at a level that justifies the costs of the system?
- Are there alternative solutions to the identified problems that would have a better ratio of benefits to costs?

1.2 Scope of the proposed system

- Identity information can be stored on the ID card as human readable and machine readable data as well as in many on-line or off-line computer data bases. A detailed specification of purpose, content and degree of cross linking of this information is essential. Note that an ID card may simplify unintentional cross-correlation between identity information held in independent databases with contentious privacy and political implications. The widespread use of the US social security number is an example of the misuse that can occur; in contrast, the implementation of the German local identity card shows how careful specification can reduce or eliminate these problems.
- Under what circumstances would a cardholder have to prove that they matched the biometric on their ID card, and what additional information about the cardholder would be called up under each identified circumstance? (This identifies a set of “required functions” for the ID system of card/ biometrics/ID database).

1.3 Fundamental specification issues

- How long could this process be permitted to take (mean, median and maximum) before the delays became unacceptable in the most time-critical of the required functions?
- What level of false positive matches (fraudulent use not detected) is acceptable for the most demanding function for which the card would be required?
- What level of false negative matches (legitimate use rejected by the system) is acceptable for the most demanding function for which the card would be required?
- What level of failure to obtain any matches (biometric not able to be read) is acceptable for the most demanding function for which the card would be required?
- Would all necessary data about the cardholder be contained on the card itself, or would there need to be interrogation of one or more databases?
- How would the authenticity of the data on the card (or in any associated databases) be established initially? What is the acceptable error rate in this data?
- How sensitive (private/secret) is the data on the card or on any associated database? (This will influence the necessary security mechanisms).
- Will any databases be accessible from public terminals or connected to the Internet?
- How many people/locations will need to be able to read the data on any databases?
- How many people/locations will need to be able to alter the data on any databases?
- What mechanisms are required to allow the cardholder to have access to, or to modify, any or all of the data held about them?

1.4 The feasibility of biometric identification

The Home Office draws on a feasibility study to show that a nationwide biometric ID card system could be implemented. The study has been published at http://www.homeoffice.gov.uk/docs2/ feasibility_study031111_v2.pdf. We believe this is a competent study and we support its conclusions, with the caveat that the analysis of error rates for the only biometric that appears to be feasible for the envisaged system (iris scanning) have been drawn from two sources of limited dependability. The first is a study of only 200 volunteers, a sample unrepresentative of the general population: http://www. cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf. The other is a study by the company that holds the patents for the technology and which would be a major beneficiary of any widespread introduction of iris scanning systems.

We believe that a well-controlled, independent, large-scale study should be undertaken before any decision is made to commit to a particular biometric technology, to ensure that the necessary low error rates can be achieved for a population of 60 million people, and that no minority group is unacceptably disadvantaged by the chosen biometric.

1.5 The feasibility of building the proposed system

In principle, there should be no insuperable technical challenge in constructing a database that could handle the likely volume of queries with acceptable performance and resilience. In practice, we have deep scepticism about the Home Office’s ability to specify, procure and implement a national, software intensive system on the scale that would be necessary. We are aware of the improvements made through the OGC Gateway process, but we see nothing in that process which would deal with the engineering complexities of this (or any similar) project, and enable the procurement to proceed at

reasonable levels of risk.

Again and again, major public-sector IT projects overrun and are cancelled, or fail to deliver the expected benefits; recent examples include systems at Post Offices, the Passport Office, the Courts, and the Child Support Agency[1]. UKCRC believes that a major factor in these failures is the unwillingness of Departments and of major IT suppliers to accept that developing software-intensive systems is an engineering task of equivalent complexity to designing a modern aircraft or building a novel sky-scraper.

Because the engineering complexity of the task is not recognised, insufficient attention is given to using the best science embedded in the strongest engineering processes (a mistake that would never be made by aeronautical or civil engineers). We believe that the quality of software engineering employed on many projects is lamentable and exposes the projects to unacceptable risks of failure; unless this problem is addressed vigorously and successfully, we believe that any national ID card system will overrun dramatically and will almost certainly fail to achieve its objectives.

2 The Security And Integrity Of The Proposed System

Security and integrity are not absolute qualities, they need to be defined in the context of the functions that the system must perform and the data that it will hold, and they need to be expressed in terms of the properties that the system must display and the allowable rate of failure for the different failure modes.

The requirements specification must include a threat analysis related to the security and integrity of the system - what are the potential failures and security attacks that can occur, what are the probability, consequences and costs of these occurring.

2.1 Availability

- For how many minutes per year is it acceptable for the system to be completely unavailable? [This could happen as the result of technical failure or following a ‘denial of service’ attack].
- What is the longest duration of any allowable loss of service for an individual function, or at an individual location?
- What will be the cost or consequence of system failures leading to longer periods unavailability than these limits?

2.2 Confidentiality

- What is the maximum number of personal database records that could be leaked by the system each year (or in total) before it was deemed too insecure to remain in operation? (even setting this limit as low as 1000 [less than 0.002% of the population] would allow the theft of the personal details of the whole membership of the House of Commons and most Premier League football players each year!).
- How many people will need access to the system and what security clearance will each person and site require? (For example, will airlines or other commercial companies need access? If so, how is it envisaged that the confidentiality targets will be achieved?)
- What level of audit trail must the system maintain, for example to allow suspicious patterns of usage to be detected? There are examples of sensitive databases that achieve a low level of unauthorised access and unauthorised modification—the Police National Computer appears to be an example where the only known leaks have resulted from bribing individuals who have authorised access, and where measures including detailed audit trails are in place to detect such leaks. We believe that the PNC is not attached to the Internet.
- What will be the costs and consequences of a major breach of the system’s confidentiality?

2.3 Integrity

- What level of barrier is needed to deter forgery of ID cards? Cambridge University have demonstrated that a moderately-equipped university research team can break the encryption of a secure commercial smartcards[2]. If the proposed ID card is important enough to justify its implementation costs, it must somehow be made secure against such attacks. Although defences can be identified for the known vulnerabilities, they are not likely to exist in current products and new

[1] See, for example, S. Pearce. Government IT Projects, Report 200, Parliamentary Office of Science and Technology, 7 Millbank, London, 2003.

[2] See http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/SISW02.pdf and related papers.

types of attack are being identified every year.
- What will be the costs, consequences and recovery mechanisms following a successful penetration of the system that leaves the integrity of the system in doubt?

UKCRC believes that any sensitive database that is attached to the Internet (or otherwise available to a large and changing population of users) will almost inevitably be successfully attacked. If the system is built on commercially available products, we do not believe that it could be made secure against intelligent, resourceful and sustained assault. The systems engineering of the proposed national ID system therefore needs to ensure that the inevitable failures will not be catastrophic or unacceptably costly.

We conclude that the amount of data stored and its sensitivity must be kept to an absolute minimum if any national ID system is to have any chance of success. If the system amounts to no more than an authenticated name-and-address directory, it will probably not be worthwhile to make serious attempts to steal or modify the data; if it goes much beyond this, it is unlikely to remain confidential, available and uncompromised.

3 Summary

UKCRC believes that:

- the Home Office should carry out a very careful Systems Engineering study to look at the costs, risks, and benefits of different approaches to meeting the overall need for a National ID system, before committing to any particular technology, to a given level of data on cards, and to the level of data available through associated databases.
- No existing system can meet the requirements, therefore it is essential that a complete and unambiguous specification of the system's requirements is drawn up, and that this specification is analysed rigorously to uncover any omissions or contradictions. We know this is technically feasible even for a system of this complexity; to fail to carry out this analysis before placing contracts would be unprofessional, and a serious waste of public funds.
- It is essential that a scientifically designed independent trial of competing biometric technologies is undertaken to ensure that the necessary low error rates can be achieved for a population of 60 million people, and that no minority group is unacceptably disadvantaged by the chosen biometric.
- Any system that is implemented will be novel, complex, and will require the use of the best available software engineering incorporating good computer science. This requires a significant change to current procurement practices but, without such changes, the project will fail.

UKCRC would be happy to give oral evidence or to answer follow-up questions on any of these points.

Martyn Thomas
for UKCRC. January 4th 2004.

Executive Summary of NAS report IDs—Not that easy.

Nationwide identity systems have been proposed as a solution for problems ranging from counterterrorism to fraud detection to enabling electoral reforms. In the wake of September 11, 2001, and renewed interest in the topic, the Committee on Authentication Technologies and Their Privacy Implications of the Computer Science and Telecommunications Board[3] developed this short report as part of its ongoing study process, in order to raise questions and catalyze a broader debate about such systems. The committee believes that serious and sustained analysis and discussion of the complex constellation of issues presented by nationwide identity systems are needed. Understanding the goals of such a system is a primary consideration. Indeed, before any decisions can be made about whether to attempt some kind of nationwide identity system, the question of what is being discussed (and why) must be answered.

There are numerous questions about the desirability and feasibility of a nationwide identity system. This report does not attempt to answer these questions comprehensively and does not propose moving toward such a system or backing away. Instead, it aims to highlight some of the significant and challenging policy, procedural, and technological issues presented by such a system, with the goal of fostering a broad, deliberate, and sophisticated discussion among policy makers and stakeholders about whether such a system is desirable or feasible.

Policy questions that the committee believes should be considered when contemplating any kind of identity system include the following:

- What is the purpose of the system? Possibilities range from expediting and/or tracking travel to prospectively monitoring individuals' activities in order to identify and look for suspicious activity to retrospectively identifying perpetrators of crimes.
- What is the scope of the population that would be issued an "ID" and, presumably, be recorded in the system? How would the identities of these individuals be authenticated?
- What is the scope of the data that would be gathered about individuals participating in the system and correlated with their national identity? While colloquially it is referred to as an "identification system," implying that all the system would do is identify individuals, many proposals talk about the ID as a key to a much larger collection of data. Would these data be identity data only (and what is meant by identity data)? Or would other data be collected, stored, and/or analyzed as well? With what confidence would the accuracy and quality of this data be established and subsequently determined?
- Who would be the user(s) of the system (as opposed to those who would participate in the system by having an ID)? One assumption seems to be that the public sector/government will be the primary user, but what parts of the government, in what contexts, and with what constraints? In what setting(s) in the public sphere would such a system be used? Would state and local governments have access to the system? Would the private sector be allowed to use the system? What entities within the government or private sector would be allowed to use the system? Who could contribute, view, and/or edit data in the system?
- What types of use would be allowed? Who would be able to ask for an ID, and under what circumstances? Assuming that there are datasets associated with an individual's identity, what types of queries would be permitted (e.g., "Is this person allowed to travel?" "Does this person have a criminal record?")? Beyond simple queries, would analysis and data mining of the information collected be permitted? If so, who would be allowed to do such analysis and for what purpose(s)?
- Would participation in and/or identification by the system be voluntary or mandatory? In addition, would participants have to be aware of or consent to having their IDs checked (as opposed to, for example, allowing surreptitious facial recognition)?
- What legal structures protect the system's integrity as well as the data subject's privacy and due process rights, and determine the government and relying parties' liability for system misuse or failure?

Each of these issues is elaborated on in the report. And each of the above questions evokes a larger set of issues and questions that must be resolved. In addition, many of these issues are interdependent, and choices made for each will bear on the options available for resolving other issues. Decisions made at this level will also have ramifications for the technological underpinnings of the system, including what levels and kinds of system security will be required. In fact, "system" may be the most important (and heretofore least discussed) aspect of the term "nationwide identity system," because it implies the linking together of many social, legal, and technological components in complex

[3] See <http://www.cstb.org/web/project_authentication>.

and interdependent ways. The success or failure of such a system is dependent not just on the individual components but also on the ways they work—or do not work— together. The control of these interdependencies, and the mitigation of security vulnerabilities and their unintended consequences, would determine the overall effectiveness of the system.

The committee believes that given the complexity and potential impact of nationwide identity systems, more analysis is needed with respect to both desirability and feasibility. In particular,

- Given the potential economic costs, significant design and implementation challenges, and risks to both security and privacy, there should be broad agreement on what problem(s) a nationwide identity system would address. Once there is agreement on the problem(s) to be solved, alternatives to identity systems should also be considered as potential solutions to whatever problem(s) is identified and agreed upon.
- The goals of a nationwide identity system must be clearly and publicly identified and deliberated upon, with input sought from all stakeholders; public review of these goals prior to selecting a proposed system is essential.
- Proponents of such a system should be required to present a very compelling case, addressing the issues raised in this report and soliciting input from a broad range of stakeholder communities.
- Serious consideration must be given to the idea that—given the broad range of uses, security needs, and privacy needs that might be contemplated—no single system may suffice to meet the needs of potential users of the system.
- Care must be taken to explore completely the potential ramifications, because the costs of abandoning, correcting, or redesigning a system after broad deployment might well be extremely high.

The legal, policy, and technological issues associated with nationwide identity systems warrant much more detailed and comprehensive examination and assessment than are presented in this report. The committee hopes that the extensive set of questions and issues raised here will help to both further and inform the policy debate. The committee welcomes feedback on this brief report as it continues preparing its broader and more in-depth final report on the topic of authentication technologies and their privacy implications.