

**Intellect Submission to the Home Office
Consultation:
Legislation on Identity Cards**

July 2004

20 Red Lion Street
London WC1R 4QN

T +44 (0) 20 7395 6700
F +44 (0) 20 7404 4119
www.intellectuk.org

Information Technology Telecommunications & Electronics Association

Contact: Nick Kalisperas, Senior Programme Manager
Email: nick.kalisperas@intellectuk.org
Tel: 020 7395 6749

1. Background

- a. This submission has been prepared by Intellect in response to the Home Office paper, *Legislation on Identity Cards, A Consultation*, which was published in April 2004.
- b. Intellect represents 1000 companies in the Information Technology, Telecommunications and Electronics industries in the UK. Intellect is committed to improving the environment in which our members do business, promoting their interests and providing them with high value services. Our membership spans blue chip multi-nationals through to early stage technology enterprises. Many of our members have been involved in similar card schemes across the world.
- c. This submission has been prepared specifically for the Home Office but draws on the views expressed in position papers written by Intellect in July 2002, January 2003 and January 2004. These papers can be found at <http://www.intellectuk.org>.

2. Introduction

- a. Intellect welcomes the opportunity provided by the Home Office to respond to this paper. This response is intended to provide an initial response to the issues raised in the draft Bill, further discussion and examination of the issues raised will be conducted through meetings between the Home Office and Intellect's ID Card Forum.
- b. Intellect once again reiterates its belief that its members and the wider UK technology industry (suppliers of cards, security technologies and integration services) have the ability to meet the technological challenges laid out by the Government's proposals.
- c. Intellect believes that it is important that all stakeholders working on the programme understand the wider ramifications of such a large IT-enabled business change programme. A fundamental understanding of the business-change issues (how processes will be affected, etc) rather than just the technological implications is crucial to the success of the programme. Intellect has been at the forefront of this work together with the Office of Government Commerce and has developed initiatives, which have sought to address the joint systemic issues around IT-enabled business change programmes. Details of these initiatives can be found at http://www.intellectuk.org/sectors/government/senior_it_forum/default.asp
- d. Furthermore, Intellect invites all suppliers wishing to participate in this work to adopt the Intellect IT Supplier Code of Best Practice, which establishes a clear set of standards that public sector clients can now expect from their IT suppliers. Intellect also invites public sector customers to familiarise themselves with the contents of the Code. Details of which can be found at http://www.intellectuk.org/sectors/government/senior_it_forum/code_practice.asp
- e. This is an extremely significant project, however, it is important that it is not undertaken in isolation. Therefore, there is a need for this work to be driven in line with other Government initiatives such as the e-Government programme and the NHS IT Strategy. Issues on data storage and manipulation arising from the Anti-Terrorism Crime and Security Act and the Regulation of Investigatory Powers Act should also be taken into account.
- f. Success will only be achieved if government continues to maintain its open dialogue with industry and engages suppliers effectively. This is something, which the Home Office, to its credit, has already undertaken, and something which we continue to welcome and encourage. The recent appointment of PA Consulting as a development partner, further strengthens this approach. Only with a comprehensive understanding of the industry, its capacity and its capabilities, will the Government develop an ID card scheme capable of delivering on its promises.

3. The Evolutionary Approach

- a. Intellect welcomes the approach taken by the Home Office during this ongoing period of consultation and deliberation. Officials have given a number of presentations to suppliers and this has enabled the development of an open dialogue between Government and industry regarding the technical issues surrounding the implementation of an ID Card.
- b. Intellect also welcomes the evolutionary nature of the proposals published by the Home Office in November 2003. The involvement of the Office of Government Commerce (OGC), with whom Intellect has an extremely productive relationship, the appointment of a Senior Responsible Owner (SRO) and the trial currently being undertaken by the Passport Service clearly point to a programme which will allow the facilitation of dialogue to ensure that the right technical solutions are adopted and subsequently implemented.

4. Achieving Adoption

- a. Modern ID programmes combine two distinct applications - e-government and secure ID on the same card. A key requirement is to balance the needs of both and ensure that sufficient attention is given to intrinsic document security and authentication, capacity of the card's memory as it relates to future-proofing and portability of data, and the potential benefits of offline operation.
- b. While UK citizens are largely familiar with authentication in relation to everyday banking transactions, the concept of an ID Card in providing routine access to government services is largely unfamiliar and the context above needs to be continually communicated to all relevant parties. Fundamental to this is the fear, uncertainty and doubt, which still exists amongst citizens concerning the introduction of ID Cards.
- c. Therefore, the success of an ID Card programme depends both on widespread acceptance and uptake by citizens, and extensive publicity of its benefits. Allied to this, the Government needs to ensure that any card is future-proof in providing sufficient data capacity, updatability and the ability to store identity information and images that cannot be erased or fraudulently altered.
- d. To succeed, the Government proposals must address the twin perspectives of citizens (citizen/consumer and citizen/taxpayer) and focus especially on citizen centric needs, including, for example:
 - The value of the card to citizens – these need to be tangible and compelling;
 - The trust of citizens in government – this must be earned and safeguarded;
 - The security of personal data – the integrity of the programme depends on this; and
 - The openness and visibility of government intentions – to overcome negative perceptions.
- e. In combination, these factors require that the Government's business proposition is substantially citizen-focussed: an ID Card will have to deliver rapid and compelling benefits to citizens to shift negative perceptions and establish the foundations for long term success.
- f. The pace at which the benefits to Government, citizens and service providers can be realised will depend on the speed with which a card is introduced and used by a critical mass of the population. The approach adopted to enrolment will be a key factor in determining the speed, cost and level of public inconvenience associated with implementation. However, it is important to state that the success of any card will be dependent on the data provided to it.
- g. Therefore, it should be possible for Government to specify and manage adherence to standards for the enrolment process and a card management scheme and card design/format, which would allow a multi-agency approach to the introduction of ID cards based on principles of interoperability and joined-up Government. This could enable exploitation of resources already in use by government and trusted third parties, in processing applications for services and entitlements, for new processes that meet the

requirements of enrolment and card issuance. It would also spread the task of population enrolment, allowing faster implementation.

5. Security, Integrity & Biometrics

- a. A universal, easily recognised form of identity that can be trusted by all, and which would involve counter-fraud measures, would obviously benefit the fight against fraud and criminal activities, but could create new vulnerabilities. To this end, it is critically important that the correct architecture is implemented which allows security schemes to evolve on the card to combat increasing levels of risk and this, in turn, relies on the quality of data available.
- b. As the Government rightly concludes there are some clear reasons why existing personal numbers issued by Government (driving licence number, National Insurance Number etc) are not appropriate, primarily because these systems were never devised to meet the need to have a unique personal number. A new unique number would need to be implemented in a way that avoids the type of problems that have occurred with other systems in the past – e.g. not attempting to link other personal data which may change, into the format of the number.
- c. Initially, under the current proposals, the card should be promoted as an identification tool, which delivers a benefit to the cardholder: a secure and reliable method of proving who they are. This will in itself improve efficiency in many areas, since the bureaucratic overhead of checking addresses, signatures, etc will be replaced by a simple and familiar mechanism. However, consideration will also need to be given to the development and implementation of cross-agency approaches as the card evolves.
- d. The design of a central database and the type of information stored will depend upon the precise characteristics of the selected ID card scheme. For example, it remains to be determined whether biometric information and PKI related data needs to be stored. However, from the papers produced by the Government, the approach outlined under which the central register stores only a minimal set of core personal information and acts, as a gateway to other Government databases seems pragmatic. It offers the potential to provide privacy safeguards surrounding the use and sharing of personal data and reduces the scale and risk of the project implementing such a system.
- e. Moreover, in the longer-term there is also the possibility that this could be extended to private sector organisations, provided that adequate safeguards are put in place to ensure that the subject's informed consent has been provided. This would provide a more comprehensive and consistent anti-fraud framework and provide tangible benefits to both public and private sectors through prevention of identity fraud related offences. Therefore, consideration should be given to the establishment of routes for verification of identity for use by commercial organisations.
- f. As noted in our previous submissions, the integrity of the ID Card programme depends upon the security of personal data. This in turn depends upon the underlying resilience and physical security of the infrastructure hardware. Protection against loss of power, physical attack and security breaches are thus fundamental to the success – and perceived success – of the programme.
- g. The National Identity Register will be a computer-based system of a scale and complexity beyond anything currently in existence. It will also be a significant asset to the Government and therefore one, which will be a target for fraudsters seeking to access the system, and terrorists (of whatever hue) seeking to disrupt or destroy it.
- h. The physical resilience of the environment in which the system is housed will be of critical importance and thus the following factors should be considered:
 - Power delivery and performance – incorporating uninterruptible power supplies
 - Environmental control – cooling and humidity
 - Fire detection and suppression

- Security and access controls
 - Specialist facility management
 - Scalable environment
 - Proximity to fibre “backbone”
 - Access to multiple telecommunication and service providers
 - 24x7 on-site technical specialists
 - Extensive back-up systems on key operational supplies
- i. Further consideration should also be given to the location(s) of the system architecture, for example:
- Will the database underpinning the national identity register be housed in a single location or several?
 - How many back-up locations for each primary one will be created?
 - What criteria will be used to determine the locations of secondary sites?
- j. Common open standards and the process to certify against these will be crucial. It is our view that the best path for Government, once it has considered these options, is to develop a specification and technical framework that suppliers can deliver against. Open published standards and interoperability are the most important criteria.
- k. It is suggested that an organisation similar to tScheme, or tScheme itself (<http://www.tScheme.org>), be empowered to develop a set or sets of criteria against which trust service providers for card systems can independently be assessed for each of the services they wish to provide.
- l. Capturing and storing biometrics as part of the enrolment process potentially offers many advantages in terms of identity verification, security and ensuring that an individual’s ‘ID card account’ remains unique.
- m. However, it is important to note that if biometric information is recorded, the selected option must meet the key criteria of being acceptable to the public and in terms of cost, viability and practicality on the scale required for ID cards.
- n. For example, the scale of the project to implement the required infrastructure could be very significant (particularly for an iris pattern biometric approach) and would need to allow sufficient national coverage to support the enrolment process and also potentially post card issue identity verification checks (on-line or off-line). The establishment of a nationwide network of biometric recording devices will need to address the issues of secure management, staff training, suitable locations and public acceptance.
- o. Further information is required for the successful development and implementation of the programme including:
- The manufacture, issuing and delivery of cards.
 - The re-issuing of lost, expired or worn out cards on a day-to-day basis.
 - If the option of a single, central database is chosen to store biometric data, will anti-terrorism measures be employed to protect such a sensitive asset?
 - Further details on the instances where ID will be checked, for what purpose, and how long it is estimated it will take to establish.
 - How will the personal ID cards of those individuals who disappear from their domestic/work situation be treated? Will cards be operational for those not considered officially dead – i.e. those missing for less than the required period of time to be considered dead.
 - How will cards be de-activated after the death of an individual- collection or central deactivation?

6. Governance

- a. The consultation document indicates the Government’s preferred option is an Executive Agency with powers delegated from the Home Secretary. Intellect believes that consideration should be given to providing an entirely new agency with this responsibility.

- b. While based as far as possible on existing card schemes, the National Identity Card would itself be a new and separate programme supported by a newly created National Identity Register. For public confidence to be maintained in the integrity of the scheme, it will be important that its responsibilities are not blurred with those of other agencies with different and potentially competing priorities.
- c. A National Identity Card Programme will need to be managed as a coherent whole since any fragmentation of responsibilities will inevitably encourage fraud and abuse to fill the gaps. It will, therefore, be essential that there should be a single agency responsible for the programme on behalf of the Government.

7. Conclusion

- a. Intellect welcomes the opportunity provided by the Home Office to participate in this consultation. Our members regard it as an important model in developing trust and cooperation between government and the private sector. It is also important to reiterate that if the project is to be implemented successfully, the Government will need to be clear on its intentions and establishes a positive dialogue with the IT industry.
- b. We also look forward to an on-going dialogue with the Home Office and other organisations about the issues raised and the technological possibilities.

Annex A

Intellect members also raised the following questions pertaining to the draft Bill (section numbers and pages refer to the Document entitled **Legislation on Identity Cards**, April 2004 ref CM 6178):

- a. p.8 Sec. 5 refers to ...existing documents (such as passport or driving licence cards). Will the Bill confirm exactly which documents will be identity cards within the meaning of the legislation?
- b. Sec.6 When will the Regulations be published, to provide details mentioned which will include technical specifications for cards?
- c. p.11 Sec.1.9 Reference is made to the opportunity for suppliers to propose innovative and flexible solutions. Will this Bill provide a framework or prescribe any limits to what these solutions may be or how the Scheme will work? If so how will these be written into the Bill or will this form part of the Regulations?
- d. p.11 Sec.1.10 What will be the timescales for formal approval of the Regulations?
- e. p.12 Sec.1.11 Can the Home Office confirm the timescale for each stage detailed herein ?
- f. Chapter 2.p.14 2.2 How will the Bill specify the biometric data? (e.g. which biometric data will be employed - fingerprint, iris or facial recognition data ?) Will this biometric be definitely held on the Register rather than on the card? We assume that choice of biometric, will be determined by the output of the UK Biometrics Trial - when will this be completed?
- g. p.15 Reference is made to verification of a person's identity by checking a card. Will the Bill define in any way how this will be achieved?
- h. p.16 Sec.2.9 At what point will the categories of information to be held on the Register be finalised?
- i. p.17 Sec.2.11 Can the Home Office confirm whether those under the age of 16 will be asked to register under the ID Scheme.
- j. p.19 Sec.2.17. Is it intended that a driving licence or a passport, doubling as an ID card, will be issued within existing renewal cycles for these documents? What will be the expiry period of each of the new designated ID documents?
- k. In general it would be very useful to understand how UK Government plan to manage the issuance, across the whole life cycle of the designated ID documents. These issues could include:
 - The management of the ID card life cycle.
 - Registration, Enrollment and initial card issuance.
 - Issuance of emergency cards and 'stopping' of lost or stolen cards.
 - Revocation of 'live' cards (owing to non entitlement).
 - Who has authority to issue cards? (e.g. Post Office, Local Council Officers etc.).
 - Authorisation for use of a card to provide access to named public services.
- l. p.28 sec. 2.69 Can the Home Office say more about how card readers will be deployed?
- m. p.33 Sec.3.9 Will Card Personalisation be required as a separate function?
- n. p.34 Sec.3.13 In the absence of compulsion what penalties may apply under the Bill for failure of an ID card holder to provide the document – will this be covered by existing powers?
- o. p.35 3.19 Would the ID (Family of) Cards be used also to access the proposed Citizen Information Register ?

- p. p.36 Sec.3.23 Will the proposed e-Passport with a facial image biometric (in line with ICAO) be issued alongside a new UK Passport ID card? Is it proposed that the ID Card Passport will be based on a Dual Interface chip also?
- q. p.37 Sec.3.24 When will the output and recommendation of the Biometric Trial be available? Will the Home Office implement the recommendations for the ID Card Family of documents?
- r. p.37 Sec.3.25 Will the biometric information be stored on the chip?