



Submission to the Access Card Consumer and Privacy Taskforce

27 July 2006

Introduction

The Access Card Consumer and Privacy Taskforce (Task Force) has released its discussion paper number 1 and asked for submissions by July 27 2006. This document is a response to this request for submissions, and represents the Development Group's advice to the Australian Government upon the subject of identification verification services.

Our response is structured into a corporate overview introducing our organisation, an alternative approach to the current thinking on the identification services, comments on the task force's identified issues and remarks on some issues with the KPMG report, followed by a conclusion.



Contents

Submission to the Access Card Consumer and Privacy Taskforce	1
27 July 2006	1
Introduction	2
Contents	3
Corporate Overview	4
An Alternative	5
The Task Force Identified Issues	6
Some Initial Questions of Principle	6
• <i>Once a Government has decided that benefits are to be paid, how do we ensure that they are paid only to those with a genuine entitlement?</i>	6
Some initial matters raised for consideration by the Task Force arising from the Government's specific proposal to date:	8
Establishing Benefits to Consumers	8
The voluntary nature of the card	8
The architecture of the access card	9
The registration and issuing procedures.	9
The need for legislative authorisation	11
Function creep	12
Using the access card and ensuring data accuracy	12
The question of balance	12
Some Specific Issues requiring further Consideration	13
Issue 1: Right of Choice	13
Issue 2: The right to and protection of privacy	15
Issue 3: Customer Benefit and Customer Control	18
Issue 4: Making the Right Technology Choices	20
Issue 5: Authorisation and Accountability	23
The KPMG report	25
Smart Cards	26
Photo Storage on Card	27
Online Access	28
RFID cards	28
Technology Scaling	29
The Private Sector	30
Conclusion	31



Corporate Overview

The Development Group is a group of associated companies that have progressively formed over the past decade to bring new technologies and business process to enable advanced electronic forms of services and methods. The Development Group was originally founded in New Zealand, but has since developed interests in both Europe and South East Asia, and we are in the progress of transforming into a global organisation.

One of our key areas of research has been the integration of novel form of database systems and card technologies to identify individuals accurately without risk of privacy abuse.

Our capability to deliver truly private systems is matched with a more efficient business case. Through economies of scope, we are able to offer services to multiple customers and thereby capture superior economics to orthodox business models. Through technology, we enable real privacy and protection for people and organisations. Through our business model, we

To date the Development Group has not approached the Australian Government regarding the introduction of unified card services for Centrelink, Medicare and other government services. It has been our impression that the Australian Government's primary focus has been upon a public sector delivery mechanism to improve service delivery and service efficiency. The Australian Government's stated intention to spend A\$1 billion upon the access card is testament to the intention to follow an orthodox business model along with its inherent costs.



An Alternative

However, we would like to draw your attention to the options that have not so far been surfaced in your discussions on the introduction of the access card and a number of underlying assumptions that have been made by both the Australian Government and KPMG regarding the state of the art of identification verification services.

First, the Australian Government can be introduced an access card without any capital outlay. The Development Group is introducing identification cards for identification verification into a number of economies around the world over the next two years. The capital investment for the identification card is covered by the identification business case.

Our original intentions were to introduce card services in Australia once we have established the service in Europe. However, we are prepared to reschedule our priorities to relieve the Australian Government of the need for card investment if there is genuine commitment by the Australian Government.

Second, our business case is based upon a transaction fee of \$1 per day, with a discounted rate for large scale transactors. This transaction fee covers all capital and operational costs of the transaction and is significantly less than the real cost that will be incurred by the Australian Government in operating the Secure Customer Registration Service (SCRS) using orthodox computer technologies.

Third, we have integrated card technologies using large-scale computing capability and bandwidth. We use large numbers of RFID readers linked by communications to our database technologies. This technological approach enables a single card to be linked independently for multiple uses, without any risk of one use affecting any other use.

Fourth, our database technology is hacker-proof. We realise that this sounds like a fantastic and implausible claim, but we have created a technology specifically to prevent unauthorised access. We guarantee that there is no way any unauthorised person can retrieve information from our database technologies without the authorisation of the card holder.



The Task Force Identified Issues

The Task Force identified a series of issues in its discussion paper number 1. The Development Group has the following position on these issues, which we have commented upon in the order in which they are listed in the discussion paper.



Some Initial Questions of Principle

- *Once a Government has decided that benefits are to be paid, how do we ensure that they are paid only to those with a genuine entitlement?*

First, we agree that the person needs to be identified. That identification should be completely accurate and the Government should not accept the potential for deliberate misrepresentation in its selection of identification capability.

Second, there is a need for service provisioning. The philosophical position of the Task Force is that benefits should be applied for before they are paid. This is a decision that has both financial and organisational ramifications. Some countries, such as Sweden, have paid universal entitlements without the requirement for request for service, thereby eliminating the need for identification of the person and their entitlement at the service centre.

Third, the service provisioning, when it is provided, can be automated to the extent that no frontdesk decisions are required. The information system can be automated to the extent that the entitlement can be automatically calculated and the service either provided or denied based upon objective measures.

The decision regarding the eligibility of government benefit is a matter of public policy.

- *A National Identity Card?*

We agree that the introduction of a compulsory national identity card is a significant erosion of personal liberties and is thus a significant degradation of the constructs of democracy upon which Australia is based. The primary concern in the United Kingdom is that the card is government controlled (40% support) rather than universal and mandatory (60% support).

However, in either case, the adoption of a card that is mandatory for accessing Government services will lead to its introduction as a de facto identification card if the card is readily usable by third parties for identification. For this reason, the Development Group believes that the Australian Government's decisions that the access card shall carry a photograph on the card and to allow the access card to become a de facto national identity card are incompatible.

- *What are the best administrative, legislative or technological guarantees which can be put in place to prevent this from happening?*

We perceive three key decisions that would assist the prevention of the access card becoming a national identity card.

First, the card should not display any photograph, signature or identification number. Any of these features will naturally lead to the use of the card as a replacement for other forms of identification within the wider community. The very nature of Government endorsement will make this form of identification superior to bank cards, student identification and drivers licences.

Second, the organisation operating the access card and database services should be independent of the Government. Independence will reduce the risk of function creep and restrict the potential erosion of protections by future governments.

Third, the agencies using the access card system to verify the identity of individuals should have independent keys for their records and should not replicate the access card data. This split of responsibility will ensure that the card does not become a proxy for a unified government profile of all citizens, and thus a frontend for a national identity system.



Some initial matters raised for consideration by the Task Force arising from the Government's specific proposal to date:

Establishing Benefits to Consumers

The Task Force has assumed that there is a balance to be struck between privacy and fraud; between customer convenience and protecting public revenue.

First, we do not think that privacy is merely a convenience. The collection of photographs and signatures opens the door to widespread and unprecedented identity theft and fraud if the information was insecure. The solution is a threat to the very Government revenues it is seeking to protect.

Second, we do not believe that privacy and Government protection are mutually exclusive. It is feasible to achieve both – but only with a trusted third party. A more pointed question is the Government is prepared to erode privacy for the purpose of state nationalisation of identification services.

The voluntary nature of the card

The pervasive nature of Government services, and the historic creep of the social state ensures that the voluntary nature of the access card is in name only. The Task Force readily admits that almost all Australians will require an access card. It is more honest to recognise the practical compulsion to carry this card, with non-card carriers becoming potentially ostracised in their interaction with government through their abstention from a pervasive system.

A defacto compulsory card needs safeguards beyond the power of any future government to erode. The only trustworthy option is a private sector partner. Nobody can honestly expect the public sector to not abuse its position as custodian and gatekeeper to services in the long term.



The architecture of the access card

We believe that the Australian Government decision is based upon obsolescent economics and technological options. The establishment of rules will not guarantee the privacy of data, and once data is released into the public arena, there is no way to regain control of the situation. Western governments have demonstrated themselves throughout history, and particularly the age of computers, as being unreliable custodians of data. The Australian Government should recognise that their system will most likely fail and it should either create risk management programmes to contain the situation, rather passing blame for a poorly engineered system upon the offender, or else implement an effective system in the first place.

There is no need to design a system with such weaknesses. The Development Group can provide an identification service that is robust, infallible and effective. It is our opinion that you should use our capabilities as the benchmark for your decisions, as any inferior system is simply unnecessary.

The Development Group can establish a secure service that can use a combination of PINs, photographs, electronic signatures, electronic keys and biometrics, based upon the desired security levels. These systems can be enhanced over time as technology develops, without the need to replace all existing infrastructure or identification cards.

The registration and issuing procedures.

The Development group offers a global card registration capability, with the supporting organisational capabilities to implement the service within the Australian government's 2008-2010 timeframe. The questions raised have already been catered for within our business case. We have addressed each question in turn.

- *How will the system deal with the problems of the vast distances and the geographic isolation of many of our people?*

Modern communications has the effect of shrinking distance. There are few places in the world and practically none in Australia that are not out of reach of modern data communications systems. The emphasis on an online database system enables people behind the identity verification service enables cost effective service provisioning at any location. The New Zealand Government is one comparable government that has elected to place its logistical systems online for the benefit of remote people.



- *How will the system deal with people who have religious or cultural objections to having a photographic record made of themselves or who, for health and/or physical reasons (e.g. certain disabilities), will be difficult to photograph with accuracy?*

The identification system should have the capability of managing multiple forms of identification. People with religious or cultural objections could elect the forms of identification that are inoffensive to their beliefs. People with disabilities or health issues can elect those forms of identity that are available for their circumstances.

The identity verification service should then respond to the demand for the variety of identification to enable sufficient access to verification to allow all citizens to access all eligible services.

- *Will the Government be in a position to provide positive and pro-active assistance to people who will need this in order to fulfil registration requirements?*

Government risk-aversion tends to make Government institutions reactive rather than pro-active. The optimal solution is to enable as many options for registration and issuance, and let the people decide what suits their circumstances. The issuance and registration service can then react to the market signals for their services.

- *How will the system deal with Australians who are resident overseas but who are eligible for, or indeed in receipt of, related benefits?*

In the case of a Development Group service, overseas people are treated locally in the same manner as local residents. In the case of an orthodox or government service, then is a reasonable expectation of a bureaucratic challenge.

- *How will people be able to establish their identity with sufficient integrity for the purposes of the access card if, for whatever reasons, they are unable to provide key primary identification documents such as birth certificates?*

The Development Group would anticipate a 99.9% success rate of verification based upon other identification capabilities. A Government service would probably be challenged to achieve significant results.



- *How will the system deal with those individuals who regularly lose their access cards and who may, in the past, have relied upon the fact that they had more than one card available to establish their entitlements? This may be a particular problem among homeless people, itinerants and in some remote indigenous communities which have relied upon their documentation being held by people other than themselves.*

Replacement cards can be charged against their accounts, thereby creating an incentive to not lose the cards in the first place,

The replacement cards can be issued based upon the data held in the database systems. The identity can be verified using database stored information, such as photographs and biometric data.

- *How can registration difficulties or procedures be minimised by making use of existing systems to establish a 'known customer' model whereby the identity of the individual in question has been established already to a required degree of satisfaction (for example, if the individual already holds a new Australian biometric passport). However this then raises a threshold question as to whether this should be allowed at all (ie would this result in the integrity of the system being reduced) or might this require inappropriate linkages of other databases?*

The existing systems all have limitations in their data collection. It is preferable to populate a database with accurate data. Data derived from other sources should be considered unverified until the registration process has been completed and the data verified as true or replaced by true data.

The alternative is to risk the integrity of the identification system based upon existing identity fraud.

The need for legislative authorisation

The use of contractual controls on a private sector third party simplifies the need for additional legislation. The Government may decide to change specific legislation in order to align it with the requirements for departments to pass information based upon an external identity verification service.



Function creep

A private sector organisation controlled by contract can be effectively controlled with the inherent conflict of interest present in the public sector. The separate of policy and operations ensures an effective control can be kept upon the scope of the service.



Using the access card and ensuring data accuracy

The Development Group's technology inherently addresses all of the identified issues. We empower the card holder as the sole person able to authorise a transaction based upon their unique identifier. We believe that other agencies should only be to access non-individual-specific data for reporting, communications or analysis.

We can protect the integrity and privacy of the data through our technology. Hackers and unauthorised access are frustrated by the nature of our database capabilities.

The question of balance

The balance sought is based upon a misunderstanding of options available, and represents a sub-optimal result for Australia. The Government has the capability to ensure real protection for citizens, protect public revenues and reduce costs while avoiding capital charges – at the cost of foregoing a nationalisation of the identification service. The question is whether the Government perception of the balance.

Some Specific Issues requiring further Consideration

Issue 1: Right of Choice

First, the integrity, accuracy and currency of the data which individuals wish to have placed upon their card can be verified by the Development Group capability. We enable a higher degree of self-verification and cross checking than feasible in normal public sector operations.

Second, we do not store the data in an open zone of the card, and we refute the requirement for such open zone data for the card to be useful. Instead, we store information on background databases accessible from any card reader. These databases ensure that open zone cards are redundant.

Third, we present our response to the questions listed in this section of the discussion paper (p. 26):

- *Noting that the Government has decided that Australian Government health and social services benefits will be paid only on production of the access card and that the consumers' right to authenticate their identity by other means may be removed, is this consistent with the required observation of the relevant Information Privacy Principles? Should people continue to be eligible to receive such benefits by establishing their identity by other means?*

The Australian Government has a responsibility to its citizenry irrespective of their identification. The denial of service to people with legitimate entitlement, whether by lack of access, lack of identification or ignorance, is not necessary a fair method treating peoples, and raises issues of public policy. Further, if a personal was able to establish their identity to at least the standards provided by an access card, then the denial of service would be merely the enforcement of a state monopoly of identification – with potentially serious consequences in the long term for the health and well-being of the Australian democracy.

- *Should people be able to obtain an access card for only limited periods of time and have the right to be removed from the relevant databases when they have completed a particular set of transactions with the agencies in question?*

People should have the right to obtain an access card for a period of time and at a later time choose to return the card and have their data permanently and irrevocably removed. Further, we believe that the person should have the right to verify that this process has indeed occurred, to eliminate the possibility of data being secretly kept for some purpose.



- *Should there be any particular rules or limitations about the data which card holders may voluntarily chose to have recorded in the chip?*

The data recorded on the card should be verified as true before it is accepted.

- *Since some of this data may be health-sensitive or for use in emergency situations it will be important to ensure that this data is correct at the time of its listing and is kept up to date—how is this to be achieved?*

Non-identification data should not be kept on the card, but rather on databases accessible through use of the card at any time.



Issue 2: The right to and protection of privacy

The Development Group places a higher regard on privacy than any Government. Our systems have been developed for the primary purpose of ensuring privacy and defeating any attack. In fact, if the Australian Government adopts orthodox technology rather than our type of technology, then we would consider it de facto acknowledgement that the statement “the Australian Government ... sets the highest priority on the introduction of the access card in a way which not only protects people’s privacy, but which uses technology which actually may enhance it” (Task Force, p. 26) as a fraud. We believe that the Australian Government has a duty, on the basis of this statement, to at the very least consider the practical ramifications of our capabilities and technologies as a counterpoint to orthodox technologies and systems.



We are ready to discuss this issue at any time.

Our responses to the questions listed in this section (p. 28) are:

- *What are the fundamental privacy issues which arise in relation to the proposed access card and would the application of the Information Privacy Principles be a sufficient guarantee that they have been addressed?*

The fundamental privacy principle in any identification system is the ownership of the identity. Copyright law generally places ownership of information with the collector of the information. This is a transfer of information from people to an organisation and represents a form of usurping property – in this case identification information. In the case of an access card, which has the potential of becoming a de facto identity card regardless of Government intentions, and enables access to multiple other services, placing the property right to the information contained on the card with the individual card holder ensures that they retain the right to use or not use their property, as they deem fit. Further, the use of this property by a third party without permission would be a usurpation of property rights and provide grounds for criminal prosecutions. An access card both opens the potential for massive and widespread identity theft, while at the same time creating an opportunity for people to asset their identity. The ownership of the identity information is crucial to the outcome. The Information Privacy Principles are inadequate for this purpose.

- *Are there special and additional matters to be considered given that the access card will involve the collection and storage of biometric information?*

The information stored on the card should be stored in such away as to render the information illegible to any party without the appropriate keys to unlock the information.

- *What role should the Privacy Commissioner play in relation to the operations of the access card, and would this role be any different from the role played already in relation to the cards which the access card is proposed to replace?*

The Privacy Commissioner role is primarily to enable people to seek adjustments of information on databases owned by organisations. The recognition of the property right of the card holder for their identification information would negate the need to extend the Privacy Commissioner's powers. If such a property right was not recognised, then the Privacy Commissioner would need the powers to reinstate somebody's identity in those cases where their identification information has been changed or deleted by third parties, including Government agencies.

- *Similarly, what role, or enhanced role should be played by the Commonwealth Ombudsman?*

We do not perceive a need to change the status of the Ombudsman.

- *Should there be a specific body created to oversight all the operations of the access card, including privacy and should this body be sufficiently independent from Government?*

The operations of the access card should be separated from the departments using the access and needs to be independent from Government in order to avoid erosion of protection mechanisms in the long term. It is our opinion that Government ownership is incompatible with this requirement and that the operating organisation should be a private sector organisation.

- *Are the existing legislative provisions relating to personal privacy adequate in the light of the access card proposal (both the principles and the proposed technology) or do they require amendment?*

The recognition of property rights for people's identification information can be granted by contract rather than by legislation. In general terms, the Information Privacy Principles are inadequate in that they are based upon the concept of corporate ownership of identity information. The existence of the Privacy Act 1988 itself legitimises a degree of information sharing that would otherwise be potentially illegal under common law. The Information Privacy principles were not designed for a world where single databases held often in a different country from the individual provided information critical to the individual's position in society. In general, the very nature of Australia being able to protect the



privacy of its citizens by declaring a set of local principles in quaint. The information world has move to a global forum, and Privacy Laws have to date proven inadequate to protect against loss of privacy from the actions of commercial organisations and governments.

- *How should the on-going operations of the access card be measured against best privacy protection practices and observation of the Information Privacy Principles?*

The Information privacy principles do not represent best practice except in their own context. The agencies requiring verification if the identification of the individual can provide services without tying personal information to the service record. If the agencies operated solely through a client record identification without the ability to identify each person without resorting to the identification verification service, then the potential for abuse of personal information within departments would be significantly reduced.

- *Are there specific classes of people (e.g. people with certain disabilities or religious beliefs) who should be allowed to have some variation in the nature of the access card which they have? If so, what variation would be appropriate?*

Everyone will need the right to an access card. People without an access card risk becoming a second-class citizen over time. A single card capability needs to be flexible enough to cater for the varying needs for identification. We believe that each card holder should have the option to tie additional information, such as forms of biometrics, to a card as alternative forms of identification for those occasions where those identification techniques are available. The provisioning of alternative methods to read the person's identity in a government service office is a technical answer to a public policy question, relating to the rights of Australians to not be disadvantaged due to religious beliefs or physical status. Multiple identification options can be located in each government office for a modest investment. Human rights have a cost and the government at least has a duty to meet that burden.

- *How can Australians be confident that new databases are not being created or new linkages created without their knowledge and consent?*

The separation of the identification verification service and its control by regulation and contract can lead to confidence that the Government will not muse the identification information for purposes beyond the original intended purpose. The recognition of the property rights of card holders for their identification would further reinforce the card holder's position, and thus lend itself to confidence that the databases are not being abused.



Issue 3: Customer Benefit and Customer Control

The task force has stated that “it is proposed that when personal details ... change, card holders will be able to have these changed in the SCRS and this will translate across all the agencies with which they have an established relationship” (p. 29). The assumption behind this statement is that the various agencies require duplicate identification verification information their records.

First, replication of information from the SCRS into the different agency databases will enable the current levels of identity theft and fraud within these agencies to continue unabated. In fact, as the records would be identical to other agency records,, a premium may be placed upon these records, resulting in creased levels of identity theft and fraud with the agencies.

Second, it is unnecessary. An alternative is that each agency can access the SCRS when and only when they require the records. In this manner, the data is held only in one organisation, there is no potential for abuse in the interim within the agencies and the card holder has the control over the use the use of their details by the nature of their holding of the card.

An identification service can be structured to enhance privacy and customer control over their identity. This service would have significant social benefit.

Our answers to the individual questions in this section (p. 29-30) are:

- *Does the proposed new access card genuinely enhance service to customer?*

The card can speed up transaction at the point of service. However, the real benefits of identity protection and privacy require that the agencies not hold personal records but instead access the SCRS when required, and only in circumstance where either the card holder has requested service or a non-individual-specific service action is being performed by the agency.

- *Does the proposed new access card genuinely enhance the right of customer choice and customer control in relation their own affairs?*

The proposed card makes little difference, and could in fact erode privacy and identity protection by streamlining the information within the agencies. The rights of customer control and choice can be enabled if the agencies did not hold duplicate identification information, but instead accessed the SCRS when authorised by the card holder or when undertaking a non-individual-specific service.



- *If there is only one card required, and that card is lost, stolen or destroyed, how can the card holder ensure there is a rapid replacement and no denial of proper benefits and that their benefits are not accessed by some other person in the interim period?*

If a card is lost or stolen, then any other person should not be able to access the service due to their failure to meet identification requirements. The person who has lost or destroyed the card can be identified from photographic and biometric information and a replacement card issued.

- *Will the arrangements for establishing proof of identity for the issue of the access card in the first instance be of sufficient integrity while at the same time not being unduly burdensome for the vast majority of Australians?*

The Development Group has created process that would prove unburdensome for most people on the planet. The arrangements of other organisations are dependent upon their customer orientation and procedures.

- *What special measures may need to be adopted if primary documents such as birth certificates are not available? In many cases these documents may have been lost or destroyed, or primary records may be held overseas and difficult to access.*

The primary records are held on Government and other databases. These records need to be accessible in order to provide the identity profile. The Development Group is implementing a global system to access similar records, thus enabling a single international identity verification capability. An Australian-only organisation could access our records in instances where local records are inadequate.



Issue 4: Making the Right Technology Choices

Technology is not a static situation. Technology changes continuously. The Australian Government selection of a technology to support the identification service is unfortunate, in that it eliminates superior options within the 2008-2010 implementation timeframe.

Further, the choice selected represented the most suitable choice only around the mid-1990s. The risk aversion inherent in the governmental decision-making process has led the government to select a technology that is (1) expensive; (2) limited in capability; and (3) obsolescent.

The Development Group predicts that by 2010 it will be apparent that the selected technology will have been superseded. We believe a better course of action is to either (1) proceed to tender for a service based upon options available; or (2) engage two or three different technological options in trials to preserve the technological choice until the decision for implementation.

Our answers to the specific questions in this section (p. 31) are:

- *Given that technological progress is so rapid these days, how can we best ensure that the access card uses proven technologies—at all levels and all stages of the access card's operations—and does not become outdated quickly?*

First, the two requirements of 'using proven technology' and 'does not become outdated' are irreconcilable. Any proven technology is by its nature several years old, and in all likelihood, no longer production. The Government needs to move beyond its risk aversion and accept the reality that any implementation using current technology is unproven.

Second, the government need not be involved in technology selection. The service can be defined in terms of required functionality and a service provider can be engaged to provide the appropriate technology, taking advantage of progress as it becomes available. In this manner, the Government divorces itself from the risks of technology selection but does not prevent the benefits of new technologies from being incorporated into the service.



- *What is the range of privacy-enhancing technologies which can be identified and incorporated into the access card?*

The primary privacy-enhancing technology is the use of a database using technologies that enforce privacy, instead of orthodox relational database structures that can enable illegitimate data retrieval from any party with access. The data held within the card should be stored in such a manner that it is illegible to any party without a valid transaction key, thus rendering the card useless to third parties. The card itself should enhance privacy by not displaying any photograph, identification number or signature on its exterior, thereby rendering it useless for other identification purposes.



- *How can we best ensure that a technology which was designed to do one thing does not get diverted or perverted into doing something quite different?*

It should be recognised that Governments across the western world have a poor track record of resisting the temptation of using information for purposes other than originally intended. Further, the private sector has been able to leverage off information leaked from government sources for a range of activities not originally intended. The solution is to place the information beyond the reach of Government's ability to modify. The information verification service should be independent of Government, including no Government involvement in ownership or governance, and the terms of information usage should be defined by contract.

- *Will the technology chosen be capable of supporting other applications if these are deemed to be desirable at some stage in the future?*

An information verifications service, by its nature, can support verification information o a wide range of other services. The supply of this service should be based on the card holder's approval and on the same terms as the other agencies.

- *Will the systems supporting the access card be sufficiently robust to do their job while also being sufficiently secure to prevent unauthorised use, hacking or abuse?*

Orthodox database technology is insecure by its very nature. Any determined hacker with sufficient time and resources can break into any system. The same situation applies to communications systems and individual cards. The 'proven' technology has all 'proven' vulnerable to a determined attack. The Development Group has spent over a decade solving this problem and has a range of technologies that are secure from any external intrusion. The degree of protection is dependent upon the technology used.



- *Will the card be capable of storing additional information which the card holder may wish to place upon it?*

The Development Group uses card technology that is more than capable of storing all information required to be placed upon the card. The selection of other card technology is dependent upon the technology selected. However, in general principle, so long as all card readers are online to the identification verification database, then additional information can always be accessed by enabling a key from the card.

- *Will the technology chosen be sufficiently user-friendly, e.g. to allow people to view their own records who are not technologically minded, be able to do so?*

The technology implemented needs to be sufficiently capable to provide multiple language capabilities, to support people regardless of their levels of literacy and to support the disabled. Any technology without these capabilities would create a two-class Australia based upon a technology divide.

Issue 5: Authorisation and Accountability

First, the Australian public are not fools. In order for the public to perceive that the body that is monitoring and supervising the access card to be perceived to be independent of the participating agencies, it really needs to be independent of the Government. The old adage of 'he who pays the piper calls the tune' is a truism in this case. Unless the body has independent finances, governance and ownership, then there is always the potential for manipulation behind the scenes and the Australian public would have good cause to be sceptical.

Second, the role of the Office of Access Card should be reconsidered. The operational aspects of the implementation of the access card and supporting database services would be better performed by an organisation independent from the Australian Government. The Office of Access Card should restrain its function to policy creation, monitoring and contractual management of the service provider. There is a conflict of interest in the agency being both provider and regulator.

Our answers to the specific questions in this section (p. 32) are:

- *Should the operation of the access card, or aspects of its operation, be placed specifically in legislation – if so, what aspects?*

The operations of the access card need only be placed in legislation if the access card operations are performed by a Government agency. A preferable approach is the supply of access card operations by an independent private sector organisation and for its operations to be proscribed by contract.

- *Once uses are defined and once specific uses are prohibited, how will adherence be monitored and what sanctions and penalties will be imposed for breaches—how will they be enforced?*

The technology selected and the business cases defined should be such as to eliminate the breaches of privacy and rights. However, the supervision of the operations should be undertaken by a body independent from the operational body. Any breach of property rights or privacy should be tackled within the bounds of existing criminal code and privacy law.



- *What are the appropriate accountability arrangements which need to be put in place to secure the transparency and integrity of the access card's operations?*

The identification verification service should keep complete logs of all information accesses and changes. The logs should be available to any card holder, and the card holder should be advised of any information request which they have not explicitly unauthorised. A regular audit of processes and transactions should be conducted to ensure the integrity of the system.



- *How will proper records be kept about who has accessed the card so that regular audits can be undertaken to ensure that the card is accessed only for authorised purposes by people who are properly authorised to do so?*

A full record of all transactions should be logged and maintained indefinitely to enable full auditing capabilities. These logs should be of sufficient capability to enable any transaction to be verified by the auditor.

- *What administrative arrangements are best suited to the control and oversight of the access card system and its on-going operations and will such arrangements be sufficiently independent of the participating agencies or the Government itself*

The best suited arrangement for the control and oversight of the access card system is a contractual arrangement between independent parties. The arrangement can only be independent of the participating agencies and the Government if the operational organisation is financially independent of the Government, and there is no Government involvement in ownership or governance of the organisation.

The KPMG report

The February 2006 report commissioned by the Department of Human Services from KPMG and titled Health and Social Services Smart Card Initiative (KPMG) follows the normal flow of a consultancy report, in that it approaches the issue methodically but with an underpinning series of assumptions based upon risk-aversion. After all, the first rule of consultancy is to only promote concepts that you know will work. The consequence is a dated approach based upon yesteryear's capabilities.

Second, the mere existence of the KPMG report demonstrates either a lack of capability within the Australian Government, and thereby an intention to capture additional capability through outsourcing the analysis of the access card to a consultancy firm, or the more common use of consultancy firms by governments of a risk transfer tool, whereby any long-term failure can be attributed to a reputable third-party and not borne by the officialdom. Neither of these reasons bode well for the future of the access card project.

We would expect that if the Australian Government was serious about introducing efficient and effective smart card services to transform the identification verification for major public services, then it would either engage the private sector to capitalise on private sector innovation, technological capabilities and a wider business foundation; or it would replicate the private sector with internal capabilities, accepting the lower efficiency from a smaller economic base.

Third, we with KPMG's assessment with the threshold issues identified in the KPMG report. We could dissect the report paragraph by paragraph and demonstrate methodological failings, limited rigour, internal inconsistencies and limited perspectives by the authors. However, we consider that these points are all rendered redundant by the inherent failing of the report to consider the looming role of identification services in the economy in general. Instead, we would like to highlight the basic failures of the report at the strategic level.



Smart Cards

KPMG has implied that the frontier industry in introducing identification cards is the banking industry, and thus has used this assumption for promoting banking industry technology standards for the access card. The banking industry has been moving for several years from magnetic stripe technology to a chip and pin technology, in an effort to raise the difficulty threshold for card manipulation and fraud.

However, there is widespread fraud in the banking industry. The banking industry keeps exact figures secret, with only cases involving large amounts generally being reported to police in an effort to minimise the overall cost from fraud to the banks. A conservative estimate of fraud in the United Kingdom 1 billion pounds in the United Kingdom over the last year.

The chip and pin cards were introduced into the United Kingdom over the past year have managed to reduce fraud has been reduced by an estimated 25%. However, the base growth of fraudulent activity has continued unabated and it can be expected that by 2007 the United Kingdom level of fraud will return to 2005 levels, when magnetic stripe cards were the standard card in use.

The smart card technology backed by a PIN identification system has led to increased sophistication of the criminal element and has not solved the underlying problem. The result is a type of arms race, with the defender against fraud and the attacker striving to gain dominance over the other. This type of arms race can achieve periods of temporary advantage only and can never be won.



Photo Storage on Card

The justification by KPMG for a smart card that was accepted by the Australian Government was the storage of photograph locally along with an electronic signature, along with the photograph printed on the card. Thus, a government service person can check the photograph on the card and read the chip to ensure that the card photograph has not been tampered with.

One advantage of this approach is there is no requirement for online access to a centralised database. The costs of communications can be minimised and the background system be used as an archive and an interface for other government systems. We presume that the Government's A\$1 billion financial estimate for the service do not include communications lines for retail locations such as pharmacies and doctor surgeries.

The problem with this approach is that it is technologically feasible to replicate a card with a fake identification and fake stored photograph, along with a valid electronic signature. The acknowledged concerns of KPMG that data on the card can be captured by a third party with a reader underscores the real potential for offline access of the cards to become a major security problem.

However, KPMG, in justifying the photograph to be placed on the card, state that the cost of placing card readers capable of displaying photographs into all locations would be high. We presume from this statement that there is a real chance that there will be locations incapable of reading the chip in the card and displaying the photograph. In such a case, either online access would be required to verify the photograph on the card or the agency would be forced to assume that the photograph is authentic. Yet, if it is uneconomic to install a screen capable of reading a card, then it is even more uneconomic to install a screen capable of communication to a centralised database.

We are left to assume that either KPMG is basing its ideas around some distorted or antiquated economics of card reading or there is a real potential of the access card being used solely as a photo id card – in which case, why is the Australian Government interested in spending A\$1 billion for no enhancement of capability?



Online Access

We believe the only logical answer to the problem is to only allow online readers to verify the card authenticity. In this case, a central data repository would need to be sized to handle the volume of transactions within the anticipated 30 second service delivery window.

However, if an online access is required for the identification verification service, then KPMG's arguments in favour of a photograph on the card become meaningless. There is no longer any justification. In fact, the photograph introduces the real risk that the access card will become used as a means of government endorsed identification beyond the government services, and thus breach the Prime Minister's expressed objectives of the access card not becoming a national identity card.

It is our view that placing a photograph on the card is a mistake on the grounds that it will encourage a sense of false security and undermine the Australian Government's efforts to introduce a robust identification service.

RFID cards

KPMG has not considered that RFID card readers will be widespread usage within the economy within a few years and that they are a valid alternative to the chip card.

RFID cards store information and are activated by the presence of a card reader. There have been a number of public misuse of RFID cards where people holding readers have captured personal information from people in public places without their knowledge and used that information to gain access to secure areas, commit fraud or merely play a prank.

The current RFID card technology has two basic limitations: (1) the data is insecure; and (2) the card holder does not know when their card is read.

The Development Group has developed RFID technology to overcome these two weaknesses. We can enable RFID technology that has no value to a third party and we can provide positive feedback to the card holder every time their card is accessed.

These enhancements to RFID cards, along with technological progress that enabled sufficient storage on these cards to hold photographic and identification information, provide the card holder mechanism for a highly secure online identification system.



Technology Scaling

The private sector has a chequered history in the Australian smart card segment. The ERG Group (ERG) failure to introduce a smart card system for the New South Wales transportation system has probably cast some doubt amongst officials regarding the private sector's capabilities in the identification field.

However, the real lesson from ERG is not the issue of private versus public sector, but instead of technology scaling. ERG made the common mistake of attempting to scale small systems to large size without being fully cognisant of the exponentially increasing risks inherent in orthodox technology.

In fact, the SCRS runs the same risks as ERG, in attempting to scale up systems to widespread implementation without considering the risks inherent in this process. The failure of both ERG and the Taskforce to directly address this issue has led us to the conclusion that the access card project is an expensive failure in the making. We are astounded that the Australian Government would consider throwing A\$1 billion away in such a cavalier fashion.

The Australian Government is probably unaware that there is no a single successful petabyte scale database system in the world. The US Government and Microsoft have been attempting a petabyte scale system since 1999, but have met with continuing failure. The scaling problem is real and the SCRS is sufficiently large that there will be scaling effects at work.

The Development Group is the only organisation available with the technology for a database system capable of supplying identification services for a potential twenty million people. We have developed over twenty years the technology specifically to overcome the scaling issue. We already have Australasia's most capable database system in testing in our research and development centre in New Zealand, and we will populate this database to multiple petabyte scale during the second half of 2006.

We know that the current Australian Government direction is going to run into the sorts of problems we overcame over a decade ago. The Australian Government can either take advantage of this capability or continue to follow the orthodox route with the high risk of a very public failure. In our case, we intend to introduce identification verification services into Australia within the same 2008-2010 window as the access card, and we foresee an unnecessary wastage on the part of the Australian Government. We believe it is beneficial for the Australian Government to leverage off our capabilities, but it is up to the Australian Government to waste public money, not us.



The Private Sector

On the surface, the supply of identification services to access public services and benefits is an obvious candidate for a public good.

However, appearances are deceiving.

First, any government agency is largely impervious to regulatory control. Regulatory safeguards against public organisations tend to be eroded for political benefit or as a method of reducing costs. In either case, the public sector organisation can be expected to progressively dismantle safeguards over time to reduce cost or to enable function creep.

Second, any government agency is largely impervious to contractual control. A government agency with a monopoly can inevitably obtain satisfactory contractual terms for supplying services to other government agencies or the private sector. Any period of political disinterest opens a window of opportunity for the organisation to modify its terms of business to eliminate any effect of contractual control over its business activities.

Third, identification services are not limited to the borders of Australia. The future will see an increasing merging of social services amongst many countries. The options in this world for a future Australian Government is whether to become an island of information distinct from mainstream global activities or to fully engage as part of the global economy. The problem is that no government can trust other governments with identification of its citizens without the real risk of reduction of sovereignty.

These three reasons lead to the requirement for international private sector organisations to provide identification verification services. Such an organisation needs to be trustable by governments, by the citizens and by commerce. The lack of trust in government to supply identification cards (e.g. 60% distrust in the United Kingdom) means that only a private sector organisation, able to be controlled by effective regulatory and contractual controls, can succeed in the long term.



Conclusion

We offer the Australian Government the opportunity to embark on the future of identification services today. We offer the Australian Government the choice of a being a country with leading edge capabilities rather than becoming second tier country following international trends, with so-called 'proven' technology.

You will appreciate that the more sensitive elements of our capabilities cannot be published in this potentially publicly accessible document for security reasons. If you would like to discuss this issue further, then we would welcome discussions. Otherwise, just watch and wait, because the future has a habit of becoming tomorrow's today.

