



Australian Government
Department of Human Services

5 January 2007

Overview of the first Access Card procurement process



Purpose of this overview document

The Department of Human Services (the Department) is seeking to keep the public informed about the Access Card programme and its progress. Consistent with this approach of transparency and accountability, the purpose of this overview document is to enable interested members of the public to obtain more information about the Access Card programme. This overview provides information about the request for tender (RFT) for the systems integrator for the Access Card as well as more general information about the Access Card programme as a whole and its progress.

This overview document does not provide full details of all aspects of the RFT and it is not intended to be used or relied on by commercial entities wishing to tender for the systems integrator RFT. Tenderers should instead obtain a copy of the RFT from the AusTender website www.tenders.gov.au.

Background

On 13 December 2006, the Department held an industry briefing to provide the information technology (IT) industry with background information about the proposed Access Card system prior to the tenders being released. On the same day, the Department held a second session which provided to interested parties an overview of the first phase of proposed legislation for the Access Card, and also released for public comment, an exposure draft of the proposed legislation. Invitations were extended to all groups and individuals who had earlier participated in the consultation process conducted by the Consumer and Privacy Taskforce chaired by Professor Allan Fels, AO.

The proposed Access Card legislation sets out in detail the information that is to be stored on the surface of the card, on the card's chip, and in the secure infrastructure underpinning the system. The proposed legislation details the ways in which your privacy will be protected and clearly sets out a range of prohibitions and severe penalties for breaches of privacy.

The Department is now commencing the first of a series of procurement processes to build and support the Access Card system. This document outlines the first of these processes as detailed in the request for tender (RFT) advertised to industry on 5 January 2007.

What is the health and social services Access Card?

It is proposed to introduce a single card for people to receive health and social services.

The card is planned to replace up to 17 existing cards, including your:

- Medicare card;
- Centrelink benefit and concession cards; and
- Veterans' cards.

It will be part of a secure system which provides benefits for both you and the community as a whole.

Why do we need a health and social services Access Card?

Australians have a world class health and social services system. To keep it that way, the Australian Government must continually make improvements.

Technology has significantly changed since the current cardboard cards and magnetic strip cards were first introduced.

Cards based on the old technology, such as the Medicare card, are becoming more vulnerable to fraud and identity theft.

In order to take advantage of today's more secure technology, the Australian Government is proposing to introduce a single card.

How will the card benefit me?

The card will benefit you by:

- improving privacy protection of your information;
- protecting you against identity theft;
- reducing health and social service fraud;
- improving services to you;
- allowing you to customise certain aspects of your card to your needs; and
- only having one card.

When can I get my card?

It is proposed to introduce the card from 2008, to be fully introduced from 2010.

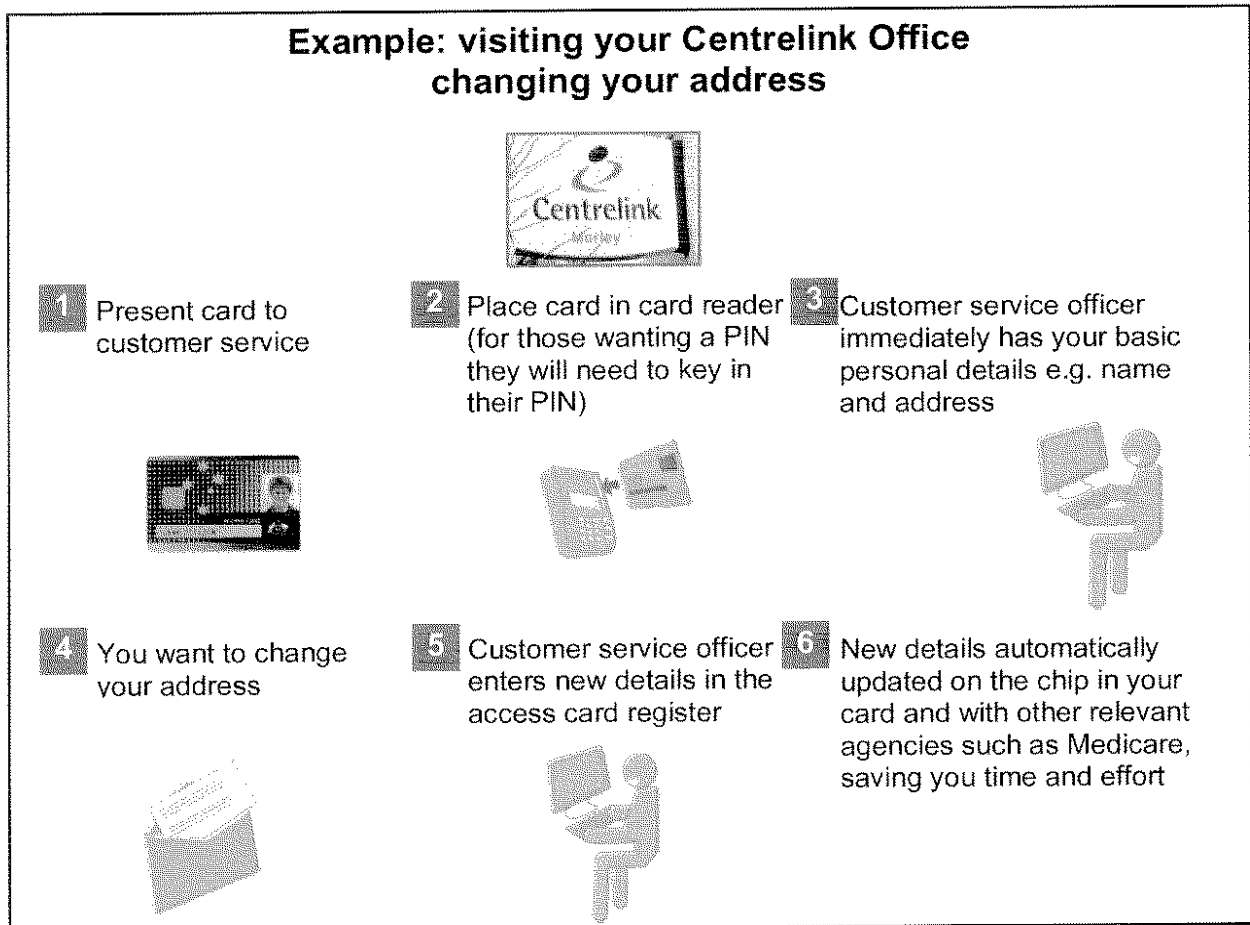
Who will the card be given to?

The card will be available to people over 18—or younger if needed—who are eligible for health, veterans' and social services provided by the Australian Government.

How will the card work?

The card will be your key to receiving Australian Government health and social services. You will need to use your card when dealing with Medicare, Centrelink and the Department of Veterans' Affairs (DVA).

It will save you time and effort.



Will my entitlements remain the same?

Yes. Existing entitlements will remain the same.

How much money is the Australian Government going to save by reducing fraud?

Up to \$3 billion will be saved from health and social services fraud over 10 years - by having a standard and secure way of verifying people's identity and eligibility to receive services and benefits.

The cost of this fraud affects every Australian.

Further Information

There is a range of information about the Access Card on the Office of Access Card website – www.accesscard.gov.au – including an *Overview of the Access Card System*; an *Overview of the Human Services (Enhanced Service Delivery) Bill 2007*; and an *Exposure Draft of the Human Services (Enhanced Service Delivery) Bill 2007*.

Also available on the website is a range of fact sheets about the card, frequently asked questions and answers, and the reports produced by the Privacy and Consumer Taskforce.

Proposed legislation

Objects of Legislation

The objects of the proposed legislation are to:

- reduce the complexity of accessing Commonwealth benefits, particularly for those who are most in need of assistance;
- facilitate a more convenient, user-friendly and reliable method of accessing Commonwealth benefits;
- reduce fraud on the Commonwealth in relation to the provision of Commonwealth benefits;
- improve access to Australian Government relief in emergency situations; and
- permit Access Card holders to use their Access Cards for such other lawful purposes that they choose.

The proposed legislation makes it clear that the Access Card will not be used as a national identity card and specifies the type of information that will be included in all areas of the card, the chip and the register.

The card

Information on the surface of the card includes the card holder's:

- name, photo and digitised signature (there may be exemptions under certain circumstances for some card holders);
- date of birth, if they request to have it included;
- card number and expiry date; and
- entitlements under the Veterans' Entitlement Act 1986, if applicable, and if the card holder so chooses, information such as Totally and Permanently Incapacitated (TPI).

People can also choose to put their preferred name on the card, if it is different to their legal name. However, the proposed legislation restricts people from using a name that is unlawful, offensive or misleading.

In certain circumstances a name will need to be abbreviated if it is too long to reasonably fit on the card.

The chip

Additional information will be stored in the card's chip, which is divided into two areas:

- the card holder's own area, which contains information controlled by them; and
- the Commonwealth's area.

Card holders can choose to protect information in either area using a PIN.

Card holder's area

The information contained in the card holder's area is optional, but could include information that would provide assistance in the event of an emergency, such as:

- health alerts, blood type or allergies;
- emergency contact details and next of kin; and

- organ donor status.

Consultation is underway with key stakeholders to determine how this information will be managed, recorded and updated on the card.

The Commonwealth's area

The information in this area is controlled by the Commonwealth and includes the card holder's:

- legal name and preferred name, if one is used;
- date of birth, if you have requested to have it included;
- gender;
- residential address;
- photo;
- digitised signature;
- card number;
- card expiry date;
- PIN, if they choose to have one;
- concession status (that is, information about your benefit cards)
- entitlements under the *Veterans' Entitlement Act 1986*, if applicable;
- Medicare number or DVA file number, if applicable; and
- reciprocal health care number, emergency payment number and other benefit card information, if applicable.

The register

To obtain an Access Card, individuals will need to apply to be registered, and to provide proof of identity documentation. Information provided by individuals when they register for an Access Card will be stored in a secure register. Information stored in the register will include:

- the card holder's legal and preferred name, if one is used;
- the card holder's date and place of birth;
- whether the card holder is an Australian citizen or an Australian resident;
- the card holder's gender;
- the card holder's address (card holders can also choose to store on the register their email addresses and phone numbers);
- the card holder's concession status (that is, information about your benefit cards or vouchers);
- the date and status of registration;
- details about the card holder's Access Card (such as its number, expiry date);
- the cardholder's digitised signature;
- the card holder's photo together with a numerical template derived from the photos;
- the card holder's DVA file number and details of their entitlements under the *Veterans' Entitlement Act 1986*, if applicable;
- scanned images of the card holder's proof of identity documents, if required;
- a flag indicating whether the card holder has a relationship with any of the participating agencies; and
- the card holder's emergency payment number (if they have one) and other benefit card information, if applicable.

Some additional information that may temporarily be held on the register as it is transferred to the chip of the card includes the card holder's:

- Medicare number, if applicable;
- DVA file number and some other DVA information, if applicable; and
- reciprocal health care card number, if applicable.

Organisation

Office of Access Card

The Australian Government announced on 26 April 2006 that it is introducing a new Access Card for use in the administration and payment of a number of health and social services benefits. The Office of Access Card within the Department of Human Services is responsible for the implementation and administration of the Access Card.

Role of the Department of Human Services

The Department of Human Services was established in October 2004 by the Australian Government to improve the development and delivery of government health and social services to the Australian people.

Human Services comprises the Department and six agencies that administer payments and services worth approximately \$100 billion to the Australian community each year. The Human Services agencies are Centrelink, Medicare Australia, Child Support Agency, Health Services Australia Limited, CRS Australia and Australian Hearing Services. Additional information about the Department and the Human Services agencies is available at www.humanservices.gov.au.

Role of the Department of Veterans' Affairs (DVA)

The Department of Veterans' Affairs is responsible for carrying out Australian Government policy and implementing programmes to fulfil Australia's obligations to those who serve or served in defence of Australia. DVA is working in close partnership with the Human Services agencies to plan, develop and implement the specific issues relating to the veteran and defence force community within the Access Card initiative. More information about the Department of Veterans' Affairs can be found at www.dva.gov.au.

Access Card procurement

Approach

To introduce the Access Card, the Department is seeking private sector contractors to build some aspects of the system. Management and control of the system will remain with the Government.

Five procurement components are required for delivery of the overall Access Card system. Each module is summarised below:

- **Systems Integration** (the scope of the first RFT) - the Systems Integrator will build and support the Access Card system and provide the training and equipment to be used for registration.
- **Registration** - registration will be undertaken by the Commonwealth using agencies such as Centrelink, Medicare and Australia Post.
- **Card production and distribution** – this will be the subject of a second tender to be released soon. This will cover the production of the physical Access Card, including putting information and the photograph on the card and its chip and distribution of the card to those who register.
- **Transaction Delivery Providers** – this will cover an accreditation process for these providers.
- **IT Infrastructure for the terminals** - this will cover the provision of card readers and terminals for the participating agencies.

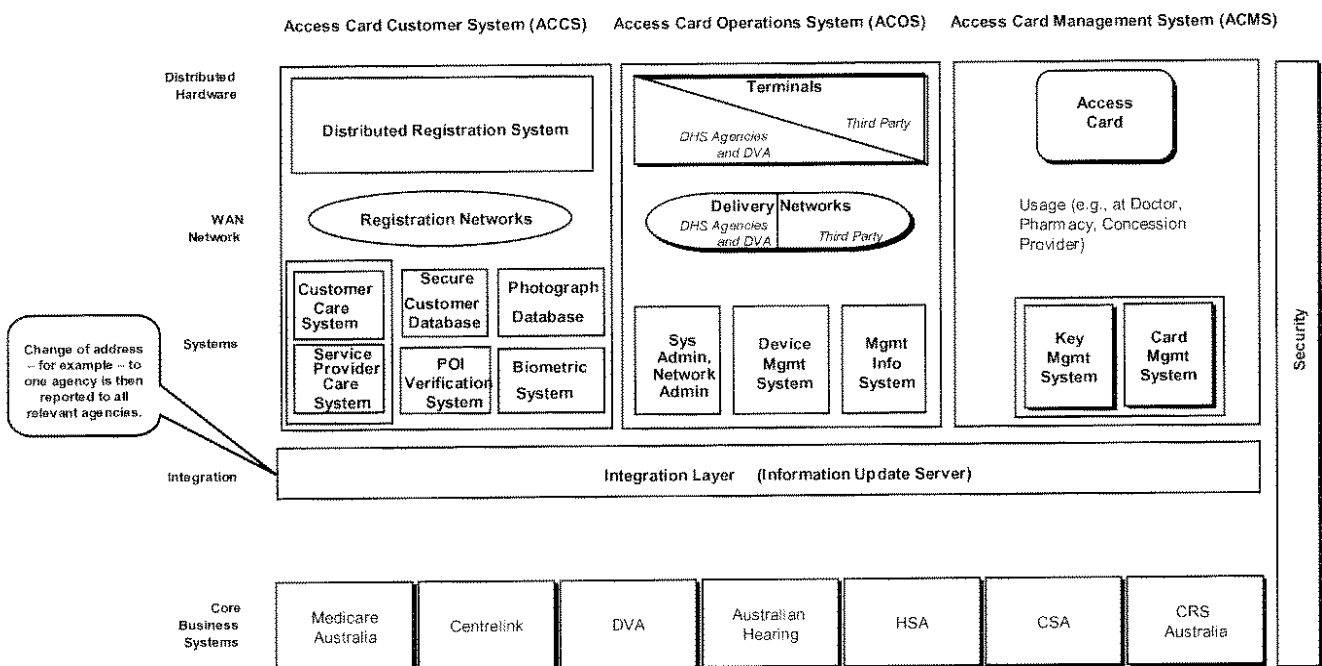
Participating agencies in the Access Card programme include Human Services agencies - Centrelink, Medicare Australia, Health Services Australia (HSA), Australian Hearing Services, CRS Australia (CRS) and the Child Support Agency (CSA) - and DVA.

Architecture

This section provides an overview of the Access Card System (ACS). At the highest level, the Access Card System comprises three parts, the:

- Access Card Customer System (ACCS);
- Access Card Operations System (ACOS); and
- Access Card Card Management System (ACMS).

Access Card Architecture



This architectural approach to the development of the access card system is a deliberate approach that enhances overall security, protects privacy, streamlines development and improves the robustness of the system.

This approach also adopts a light touch to integration with agencies' systems. The architecture does not involve – and does not require – re-engineering and deep integration with agencies' existing systems.

This approach also does not involve the creation of a mega database.

Systems integrator request for tender (RFT)

Purpose of the first RFT

The purpose of the first RFT is to engage a contractor to provide the infrastructure that supports the privacy, security, registration and operational aspects of the card that are detailed within the proposed legislation.

No mega database holding all your information

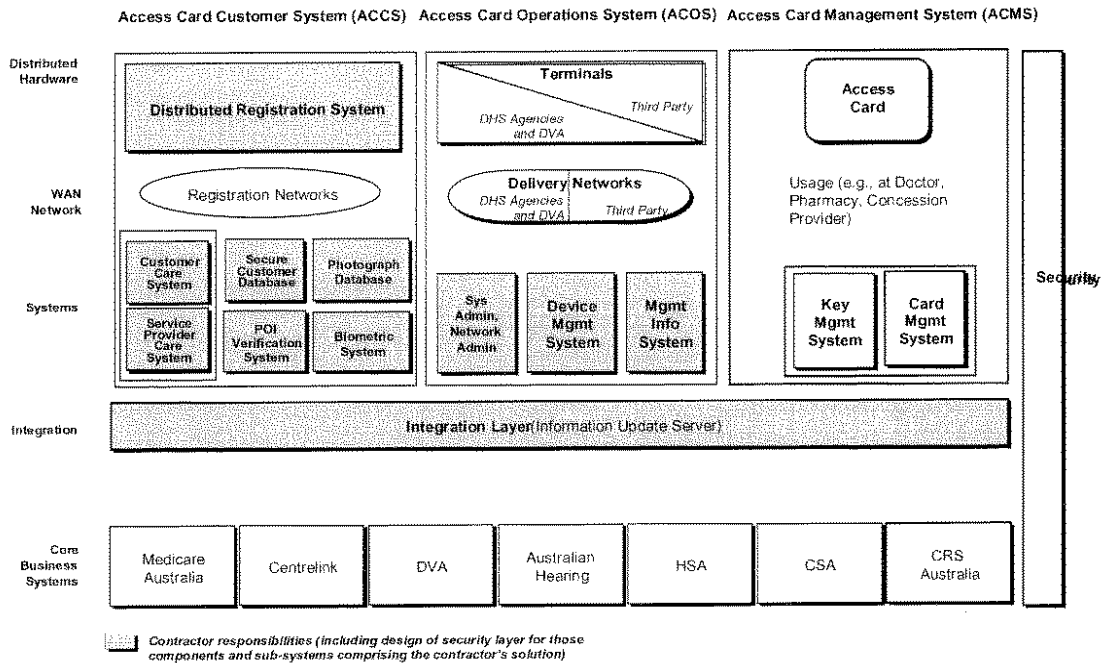
It is important to note that the Access Card system does not allow for the development of a mega database combining all the information about you currently stored within participating agencies.

Scope of the RFT

The Department is seeking tenders for the delivery of the Systems Integrator components of the Access Card system and related services. The successful tenderer will contract to deliver these components as well as provide ongoing support for at least three years after the system is accepted by the Department.

The scope of the Systems Integrator components is indicated by the shaded areas of the Architecture diagram below.

Access Card Architecture



The Systems Integrator will be responsible for implementing three key pieces of Access Card architecture:

- The Access Card Customer System (both hardware and software);
- The Access Card Operating System (data centre components); and
- The data integration layer supporting the flow of data between access card components participating Department of Human Services agencies and the Department of Veterans' Affairs.

The Systems Integrator contractor will not be a prime contractor for the overall Access Card system.

Registration process

All people accessing Australian Government health and social services benefits from 2010 will be required to register for an Access Card. It is expected that up to 16.7 million people will apply to register for their Access Card over a two year period between 2008 and 2010.

Planning for the registration process is underway and importantly will be influenced by public consultation. The Consumer and Privacy Taskforce is expected to soon release a discussion paper on the registration process for public comment. In addition, the Department is consulting with a range of stakeholder groups to determine the most appropriate mechanism for issuing cards to vulnerable groups within the community, such as those with mobility restrictions, homeless people, or those without access to proof of identity documents. Exemptions will be made for people in special circumstances.

Registration equipment requirements

It is recognised that there will be peaks in registration demand at different locations, at different times of the day, week and throughout the year. Registration capacity needs to meet demand through:

- additional registration counters and staff in existing locations;
- additional registration outlets;
- temporary locations and mobile units; and
- extended operating hours (at night or weekends).

The successful contractor for the Systems Integrator module will provide the equipment to allow people to register and will install a common system of registration.

Registration units will be installed at fixed locations (e.g. Medicare, Centrelink, DVA and Australia Post offices) and as part of mobile registration units (to support registration at remote locations). Mobile registration vehicles will be provided by the Department to be fitted out by the contractor as mobile registration units.

Security and privacy

Protecting the security and privacy of individuals' information is paramount and the Government and Department have put in place a range of measures to ensure that the legal and operational infrastructure underpinning the access card protects this information.

Legislation

The Access Card Consumer and Privacy Taskforce recommended in its first report that a comprehensive legislative framework be developed for the access card programme.

The Government supports the Taskforce's recommendation. The Australian Government has released for public comment proposed legislation that will:

- provide for the introduction of the new card to access Australian Government benefits and services;
- define information to be collected and stored on the surface of the card, the chip and the register;
- clearly set out prohibitions and protections unique to the access card;
- vest ownership of the card in the card holder; and
- address other matters to do with effective implementation of the card programme.

Most importantly, legislation will ensure that the access card is:

- not a national identity card;
- not required to be carried at all times; and
- able to be used for any lawful purpose you choose.

The Access Card legislation will build on existing laws that protect privacy and information disclosure.

Legislative protections

In order to protect the card and the information associated with it, the proposed legislation sets out a range of offences that apply for improper use of the card. Heavy penalties apply for individuals, third parties and Commonwealth officers who are found to be unlawfully using the card, or the information associated with it.

For instance, it will be an offence:

- for a person to require you to produce your, or someone else's card, other than for the purposes of the legislation;
- to do specific things to an Access Card, such as selling it, defacing or damaging it, or changing information on the Commonwealth's area of the chip, with the intention of dishonestly obtaining a benefit; and
- to dishonestly obtain an Access Card, or possess a fake Access Card.

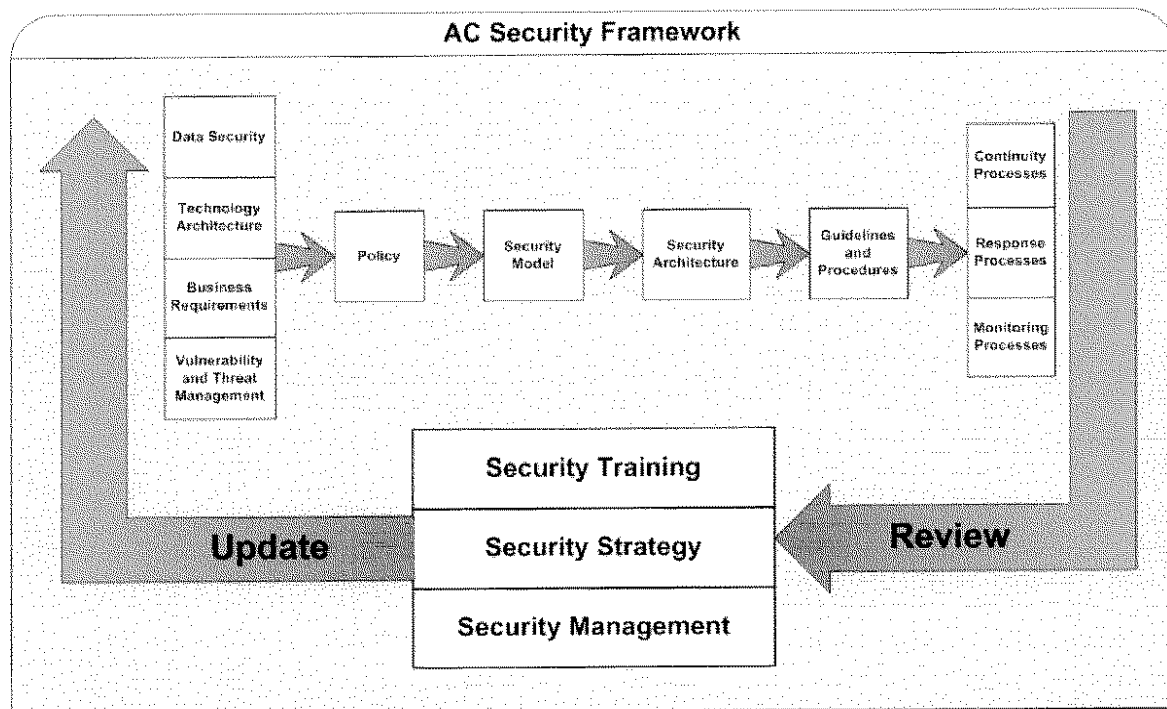
Specific offences also apply to Commonwealth officers.

Ownership

Individuals will own their Access Card. As individuals will own their Access Card, they are able to use it for any lawful purpose, including using it for identification purposes, if they choose. However, there is nothing in the proposed legislation that requires people to carry the card with them at all times, and the proposed legislation explicitly states that Access Cards are not to be used as national identity cards.

Privacy and Security Enhancing Architecture

The Department of Human Services has made a significant commitment to ensuring that security for the Access Card programme is engineered into every aspect of the programme, from the initial conception through design, and the entire life of the programme.

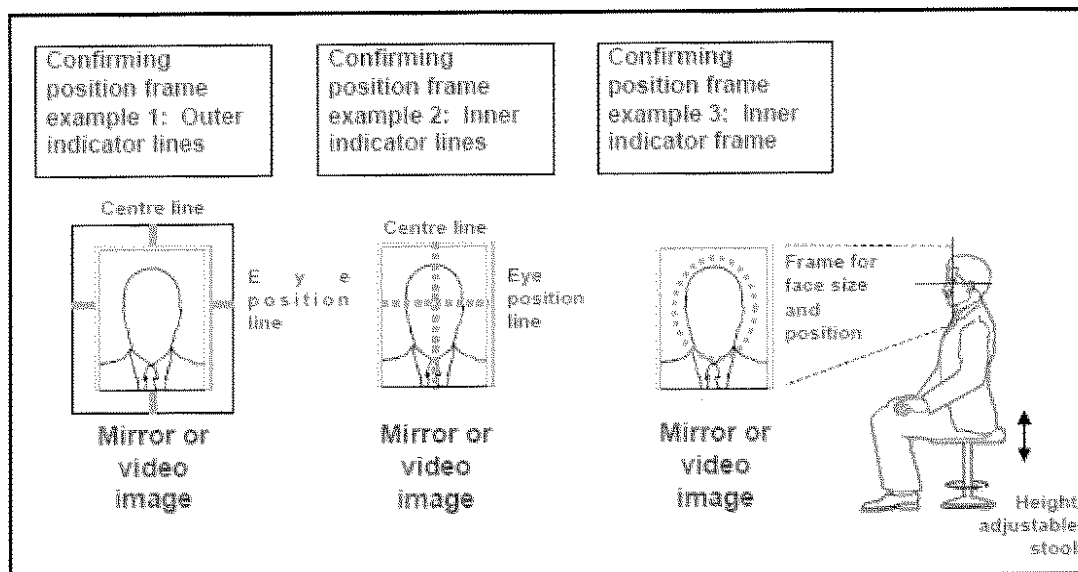


The Access Card system will use advanced and proven smartcard security technologies. This will be a significant improvement on the outdated magnetic strip and cardboard cards in use today.

Security is built into the chip and onto the card to prevent and detect tampering with the physical card, and to secure the card holder's information. To strengthen cardholder privacy, the amount of data shown on the surface of the card has been minimised. There is much less data visible on the Access Card than on any Australian drivers' licence. Importantly, your card will have on its surface your photograph. Swapping, borrowing or stealing cards will be far less attractive as your photograph is on the card, and the card will have higher security and anti-tampering features than existing cards.

Biometric technology

The security and privacy enhancing design of the Access Card system includes biometric technology. Biometrics refers to the technology that measures and analyses physical characteristics for authentication purposes. Facial biometrics is a system that compares facial photographs to find possible matches.



It should be noted that the proposed legislation provides exemptions under certain circumstances for people not to have a photograph taken and included on the card.

For the Access Card, biometric technology measures characteristics of your photograph to prevent people from trying to register twice to defraud the system.

Security on the card and in the chip

On-card physical security will use a variety of mechanisms to protect the card against tampering, and to defeat counterfeiting. These include security printing of various forms on the surface of the card, and the protection of the photograph on the surface of the card by a high quality Optical Variable Device.

Information on the chip in the card will be protected using advanced technology such as encryption, PIN protection and secure zones.

Restricting access to your information

All online activity will be securely logged, including access, authentication, transactions and business activity. All logs will be analysed constantly for anomalous behaviour. Further underlining the emphasis on security and privacy, the exposure draft legislation contains penalties for staff who inappropriately access information contained in the Access Card system.

This comprehensive approach to security and privacy ensures that the three dimensions – that of people, physical and information security – are built into every part of the solution.

Defence Signals Directorate (DSD) evaluation and certification

An important element of the security framework is evaluation, testing and certification by the DSD. The DSD is Australia's national authority for information security and signals intelligence. DSD has two principal functions: one is to provide Information Security products and services to the Australian Government and its Defence Force; the other is to collect and disseminate foreign signals intelligence.

DSD plays a key role in the protection of Australian official communications and information systems. For information that is processed, stored or communicated by electronic or similar means, the role of the DSD is:

- to provide material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; and
- to provide assistance to Commonwealth and State authorities in relation to cryptography and communications technologies.

The contractor must work with the Department and DSD to complete DSD evaluation and certification for the entire Access Card system.

No data offshore

The Department must approve the location of any stored data.

To ensure that the Department meets its privacy obligations it is the Department's policy that no personal information will be sent offshore. All encoding of blank cards will be done within Australia and all information transmitted for personalising blank cards will be encrypted and to the standard required by the DSD.

An independent audit of the physical security environment of the supply site will be completed by a DSD accredited auditor. The audit will ensure compliance with the relevant government security standards as stated in the contract.

As mentioned previously, there will be no one central database containing all the information relating to each individual card holder. Details of each individual's interaction with either DVA or a Human Services agency remains where it is currently stored – within that agency's systems.

Standards

The Access Card system will comply with applicable international and Australian standards to optimise security, interoperability and long-term maintainability. These standards are increasingly being used around the world by governments to provide more secure access to a range of services.

In addition the card data model must be consistent with the draft standard "Australian Government Smartcard Framework" available from www.agimo.gov.au and the interoperability draft standard ISO24727, Parts 1-3.

Importantly, the Access Card system, based on these standards, avoids proprietary lock-in. The comprehensive verification and certification of the design and implementation will ensure compliance with these standards.

Tender evaluation

Consistent with Commonwealth procurement policy, the Department will evaluate tenders on the basis of best value for money. Tenders for the Systems Integrator RFT will be evaluated in accordance with the following evaluation criteria:

- compliance, including privacy;
- capability;
- experience and past performance;
- financial viability and corporate capacity; and
- affordability.

Selection of the preferred tenderer will be made by the Australian Government on the basis of the above evaluation, and taking into account considerations such as national interest, affordability, strategic considerations relating to the development and implementation of the Access Card, other whole of government considerations and the level of risk posed by each tender.

Small to medium enterprise participation

The Australian Government recognises that the public sector is a significant market for small to medium enterprises (SME) in the IT industry. The RFT documentation specifically invites tenderers to describe how they will involve SMEs in the delivery of services.

In particular, the agreement requires the contractor to:

- ensure that it meets the following minimum SME participation level:
 - 10 per cent of the total value of hardware purchased;
 - 20 per cent of the total value of software and services; and
- report to the Department annually on the contractor's SME participation level.

Contractor performance

The RFT documentation contains a draft agreement that sets out a range of performance measures to ensure that individuals' information is protected and that the system remains secure. These measures also ensure that the Australian Government, and ultimately taxpayers, receive value for money through the contract.

Table 1 provides an overview of these measures.

Table 1

	Event	Department's rights and remedies under the Draft Systems Integration Agreement
1.	<p>The contractor:</p> <ul style="list-style-type: none"> - breaches confidentiality; - breaches any laws; - breaches privacy; - intentionally or recklessly commits wrongful acts; - acts negligently or unlawfully; - commits fraud; - provides materials (including software and hardware) which infringes third party intellectual property rights. 	<p>The contractor is required to indemnify the Department for any resulting claims.</p> <p>The contractor's liability for damages is unlimited.</p> <p>The Department will be able to call on the financial guarantee.</p> <p>The Department will have remedies against the contractor's parent under the parent company guarantee.</p> <p>The Department may be able to claim against the contractor's various insurance policies required by the Department (having regard to the level and cover appropriate to the nature and size of the contract) and under which the Department will be a named insured.</p> <p>The Department may also have the right to terminate the agreement and exercise rights of step-in.</p> <p>If the Department terminates, or is entitled to terminate the agreement, the Department will be entitled to retrieve the source code for proprietary software (other than Commercial off-the-shelf software (COTS)).</p>
2.	<p>The contractor fails to meet a service level or key performance indicator.</p>	<p>The Department may be entitled to claim service credits attributable to that failure.</p> <p>The Department will have the right to claim an appropriate level of damages.</p>
3.	<p>The contractor is late in meeting a milestone, other than due to an event out of the control of the contractor.</p>	<p>The contractor must provide reports indicating the nature and extent of the delay and the work-arounds that it is to implement.</p> <p>The contractor must pay liquidated damages for each day of delay. The contractor may also be liable for damages for default. The Department will be able to call on the financial guarantee.</p> <p>The Department will have remedies against the contractor's parent under the parent company guarantee.</p> <p>The Department may be able to claim against the contractor's various insurance policies required by the Department (having regard to the level and cover appropriate to the nature and size of the contract) and under which the Department will be a named insured.</p> <p>If the contractor does not remedy the delay within five business days of notice requiring it to do so, the Department may terminate the agreement or exercise a right of step-in.</p> <p>If the Department terminates, or is entitled to terminate the agreement, the Department will be entitled to retrieve the source code for proprietary software (other than COTS software).</p>

4.	The contractor otherwise breaches the agreement.	<p>The Department will have the right to claim an appropriate level of damages.</p> <p>The Department will be able to call on the financial guarantee.</p> <p>The Department may have remedies against the contractor's parent under the parent company guarantee.</p> <p>The Department may be able to claim against the contractor's various insurance policies required by the Department (having regard to the level and cover appropriate to the nature and size of the contract) and under which the Department will be a named insured.</p> <p>The Department may have the right to terminate the agreement and exercise rights of step-in.</p> <p>If the Department terminates, or is entitled to terminate the agreement, the Department will be entitled to retrieve the source code for proprietary software (other than COTS software).</p>
5.	The contractor becomes insolvent or ceases, or threatens to cease, to conduct business.	<p>The Department will be able to call on the financial guarantee.</p> <p>The Department will have remedies against the contractor's parent under the parent company guarantee.</p> <p>The Department may be able to claim against the contractor's various insurance policies required by the Department (having regard to the level and cover appropriate to the nature and size of the contract) and under which the Department will be a named insured.</p> <p>The Department will have the right to terminate the agreement and exercise rights of step-in.</p> <p>If the Department terminates, or is entitled to terminate the agreement, the Department will be entitled to retrieve the source code for proprietary software (other than COTS software).</p>
6.	Contractor walks away from the project.	<p>The Department can bring a claim against the contractor for default under, and repudiation of, the agreement. The contractor's liability is unlimited.</p> <p>The Department will be able to call on the financial guarantee.</p> <p>The Department will have remedies against the contractor's parent under the parent company guarantee.</p> <p>The Department may be able to claim against the contractor's various insurance policies required by the Department (having regard to the level and cover appropriate to the nature and size of the contract) and under which the Department will be a named insured.</p> <p>The Department will also be entitled to exercise a right of step-in and to terminate the agreement.</p> <p>If the Department terminates, or is entitled to terminate the agreement, the Department will be entitled to retrieve the source code for proprietary software (other than COTS software).</p>

Warranties

The Department will require from the contractor performance related warranties and representations to the effect that:

- the solution and services will be fit for the purposes described by the Department;
- it will supply the solution and services promptly, diligently and with due care and skill;
- it will have at the relevant time the necessary resources;
- the solution will not contain any harmful code; and
- it will provide the solution and services in accordance with all laws.

Licence rights for the contractor software

The Department will obtain from the contractor appropriate non-exclusive, worldwide, perpetual, irrevocable, royalty free rights to use Intellectual Property (for example software) for the purposes of the Access Card programme including for back-up and security purposes.

Timetable

The proposed timetable for the first RFT process is set out in the table below:

Event (indicative only)	Proposed Date
Issue of RFT	5 January 2007
Closing time for RFT	5pm 1 March 2007 (local Canberra time)
Presentations and site visits (if required)	To be determined
Notification to preferred tenderer(s)	Late April 2007
Negotiation of draft agreement	Early May 2007
Signing of agreement	Early May – June 2007
Design phase complete	Early July 2007
Development phase complete	Mid-November 2007
Australian Government security evaluation commences	End November 2007
System testing complete	Mid-January 2008
Australian Government security evaluation complete	March 2008
Commence call for applications for registration	March 2008
Registration process commences	April/May 2008

Next steps

To ensure that community and stakeholder views are considered throughout the development of the Access Card programme, consultation with a range of groups is continuing.

The Consumer and Privacy Taskforce will release its discussion paper on registration for public comment. This will be available through the Access Card website – www.accesscard.gov.au.

A second RFT will follow soon for the card manufacture and distribution. Details of the first RFT will be available on AusTender and an overview document, similar to this document, will be available on the Access Card website.

Information on the website is updated regularly and is a primary source of information about the programme. People interested in the ongoing development of the programme, or who wish to provide comment on discussion papers can do so through the website www.accesscard.gov.au. An information line – 131 792 – is also available for further information.