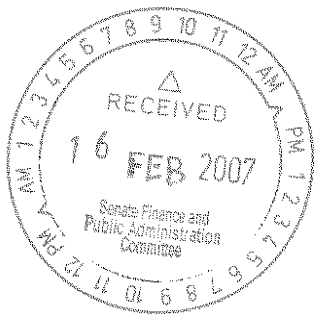
Australian Government
Department of Human Services



31 January 2007

Overview of the second access card procurement process

CARDS ISSUANCE AND MANAGEMENT

Purpose of this overview document

The Department of Human Services (the Department) is seeking to keep the public informed about the access card program 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 program. This overview provides information about the request for tender (RFT) for card issuance and management for the access card as well as more general information about the access card program as a whole and its progress.

This overview document is not intended to be used or relied on by commercial entities wishing to tender for the Card Issuance and Management RFT. Tenderers should instead obtain a copy of the RFT from the AusTender website, www.tenders.gov.au, after having completed the confidentiality requirements set out on the AusTender website.

More than 150 pages in the tender documentation are dedicated to detailing the Department's requirements, and specifying performance standards for the access cards and for other systems that will support and secure the cards. A further 150 pages detail the Department's requirements and set performance standards for the contractor.

The contract involves cards being sourced from multiple suppliers. This is international best practice and takes into account overseas experience. The Department is reducing its risks by having more than one supplier of cards.

Intentionally, not every detail of every requirement is specified. In some areas, tenderers may suggest different ways of doing things. The Department will consider various possible approaches and select the best one. In this way, it fosters competition to deliver the best value for money solution consistent with maintaining security and privacy.

Background

There is a legislative framework for the access card, and the Access Card System (ACS) will operate in accordance with legislation and strict guidelines. An Exposure Draft of the first package of legislation was released for public comment and is available on www.accesscard.gov.au.

The proposed legislation sets out in detail the information visually identifiable on the surface of the card, in the card's chip, and in the secure infrastructure underpinning the system. The proposed legislation details the ways in which people's privacy will be protected and clearly sets out a range of prohibitions and severe penalties for breaches of privacy.

On 13 December 2006, the Department of Human Services (the Department) held an industry briefing to provide the information technology (IT) industry with background information about the proposed ACS prior to tenders being released. On the same day, DHS 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 Department has commenced a series of procurement processes to build and support the ACS.

The first Request for Tender (RFT) – the Systems Integrator RFT – was released on 5 January 2007. The Department is now releasing the second RFT for the Card Issuance and Management.

This document outlines this second RFT as detailed in Card Issuance and Management RFT for the access card released to industry via AusTender on 31 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:

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

It will be part of a secure system which provides benefits for individuals 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 individuals?

The card will benefit individuals by:

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

When can people get a card?

It is proposed to introduce the card from April 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 the key to receiving Australian Government health and social services. People will need to use their card when dealing with Medicare Australia, Centrelink and the Department of Veterans' Affairs (DVA).

It will save people time and effort.

Example: visiting your Centrelink Office changing your address

1. Present card to customer service

2. Place card in card reader (for those wanting a PIN they will need to key in their PIN)

3. Customer service officer immediately has your basic personal details e.g. name and address

4. You want to change your address

5. Customer service officer enters new details in the access card register

6. New details automatically updated in the chip in your card and with other relevant agencies such as Medicare, saving you time and effort

Will individuals' 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.

Proposed legislation

Legislation has been proposed for the access card and on 13 December 2006, an Exposure Draft of the *Human Services (Enhanced Services Delivery) Bill 2007* was released, allowing for full public consultation and comment on the proposed legislation.

Submissions on the exposure draft closed on 12 January 2007. The Office of Access Card received over 120 submissions from organisations and individuals. These submissions are the subject of active consideration prior to the finalisation of the Bill. It is expected that the Bill will be tabled in Parliament by the Minister for Human Services in the near future.

Further Information

There is a range of information about the access card and the proposed legislation on the Office of Access Card website: www.accesscard.gov.au. This includes an *Overview of the Access Card System* (the first procurement process); an *Overview of the Human Services (Enhanced Service Delivery) Bill 2007*; and an *Exposure Draft of the Human Services (Enhanced Service Delivery) Bill 2007.* Submissions in response to the Exposure Draft are also available on the website.

The website also has a range of fact sheets about the card; frequently asked questions and answers; and reports produced by the Consumer and Privacy Taskforce.

Organisation

Office of Access Card

The Australian Government announced on 26 April 2006 that it would introduce 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 is responsible for the implementation and administration of the access card.

Role of the Department of Human Services

The Department 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.

DHS 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 (DVA) is responsible for carrying out Australian Government policy and implementing programs 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 DVA can be found at www.dva.gov.au.

Access card procurement

Approach

To introduce the access card, DHS 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 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 Australia, DVA and Australia Post.
- **Card Issuance and Management** – (the scope of this RFT) - this will cover the management system for the access card and the security keys, 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 (including terminals)** - this will cover the provision of card readers and terminals for the participating agencies.

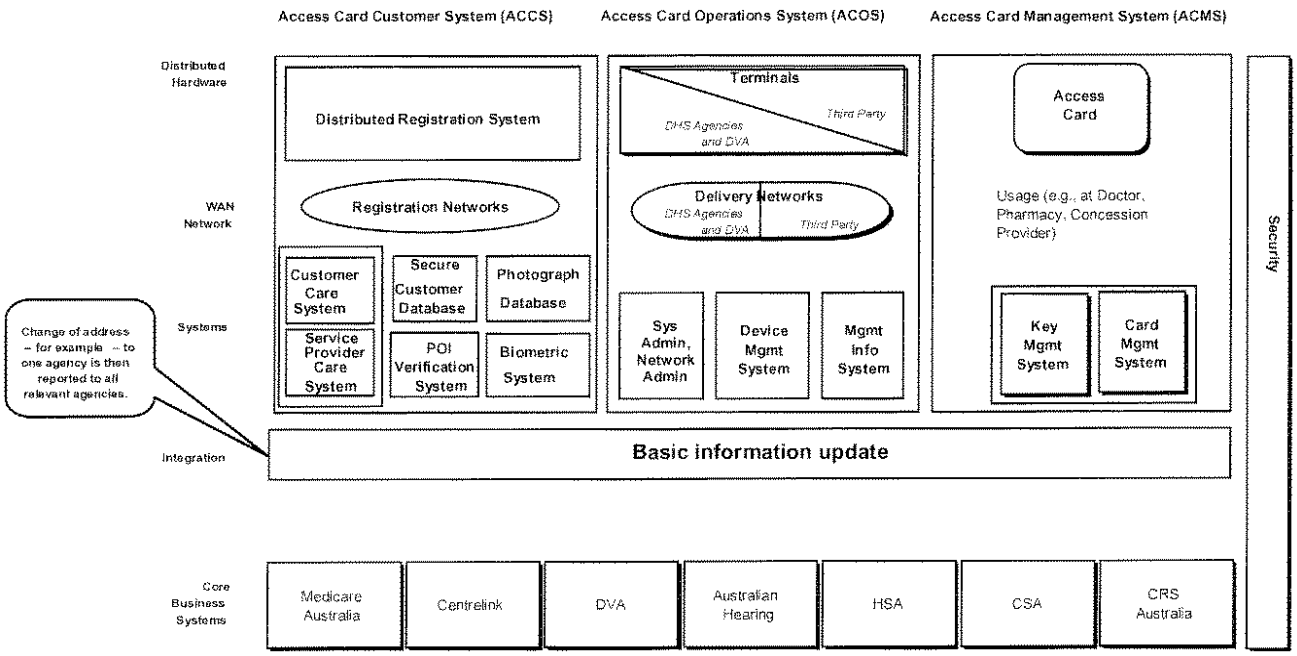
Participating agencies in the access card program include Human Services agencies - Centrelink, Medicare Australia, Health Services Australia (HSA), Australian Hearing Services, CRS Australia (CRS) and the Child Support Agency (CSA) - and DVA.

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 Management System (ACMS).
    - The Access Card Management System (ACMS) comprises two core components - the Card Management System (CMS) and the Key Management System (KMS) - in addition to the access cards themselves.

Access Card System



This architectural approach to the development of the ACS 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.

No mega database

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

Systems integrator Request for Tender (RFT)

The first part of the access card procurement process is the Systems Integrator RFT which was released on 5 January 2007. The purpose of the first RFT is to engage a contractor to provide the infrastructure to support the privacy, security, registration and operational aspects of the access card that are detailed within the proposed legislation. The systems integrator and the card issuance and management prime contractor will be required to work very closely together. Importantly, the systems integrator is responsible for end-to-end testing including those components delivered by the cards issuance and management prime contractor.

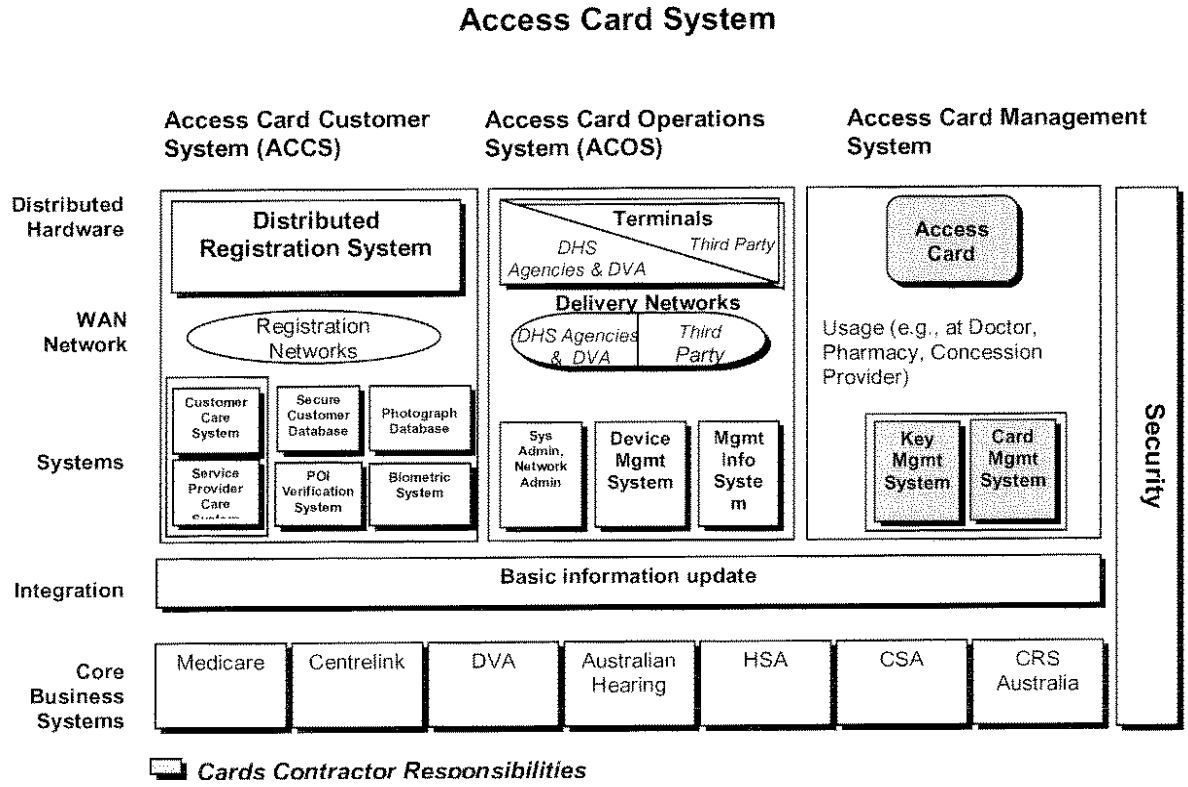
Access Card Issuance and Management Request For Tender (RFT)

Scope of the RFT

The Department is seeking tenders for a prime contractor to implement a cards and key management system. Also, the tenderer will be responsible for the design, manufacture, initialisation, personalisation and distribution of the access card.

The successful tenderer will contract to deliver these components as well as providing ongoing support for at least three years.

The scope of the card issuance and management contractor's responsibilities is indicated by the shaded areas of the architecture diagram below.



The successful tenderer will be responsible for implementing the three key pieces of access card architecture:

- The access card;
- The Card Management System; and
- The Key Management System.

Access cards

Access cards will enable the cardholder to access benefits and services from participating government agencies.

The access cards themselves are the components that are most visible to the general public. The cards will have, on the surface of the card and in the chip, basic information about the cardholder (for example, name, and optional date of birth). In addition, information about their dependants, concession status and entitlements will be in the chip. The card and the chip will also have a photograph of the cardholder and a digitised signature.

The cards must be able to withstand daily wear and tear, and must be robust and secure. The cards must be designed to protect cardholder's information and will include anti-counterfeiting and anti-tampering technology, as well as multi-level security. The successful tenderer will be asked to provide a proposed approach for ensuring the environmental impact is minimised from production to destruction of the card – that is, throughout the card life cycle.

Contracting approach to the supply of the access card

The contracting approach to the supply of the access cards is to divide the supply into three separate supply components:

- Supply of smartcard chips;
- Supply of blank card stock; and
- Card personalisation and issuance services.

Different suppliers in different locations are required to supply the components. This is to protect against a bottleneck or other disruption in the supply of access cards, especially physical and financial risks in connection with supply (such as a physical disaster or insolvency on the part of one of the suppliers).

For each component of the supply, the tenderer will be required to make arrangements for:

- At least two suppliers;
- Suppliers not to share premises; and
- No single supplier to supply more than 60% of the annual requirement.

The Card Management System (CMS)

The Card Management System (CMS) will manage and track access cards through their entire lifecycle - from manufacture through to personalisation, registration, delivery, usage, updates to data or applications and retirement.

For example, the CMS will be the system used to create new cards for individuals and record the issue of replacements for lost or stolen cards, and will also enable the data in the chip to be updated by authorised people. The CMS will also monitor how many cards are issued so that stocks of new cards are readily available.

The chip in each card will have a number of software applications on it. These applications will assist the secure storage and transfer of relevant information. Part of the CMS will also comprise an application management system. This system will be able to manage the different applications on the card and could be used, for example, to update certain encryption parameters in the card to enhance security. This process can happen online when an access card is used (for example, when the card is presented and docked in Medicare Australia or Centrelink offices).

Cards and the CMS must be able to securely communicate with other ACS modules.

Key Management System (KMS)

Encryption keys will be used to securely communicate between elements of the ACS. These keys will provide the mechanism by which data is protected on the access card chip and will ensure that only authenticated devices are able to read and update information to the chip. The KMS will manage encryption keys, including the creation or reception of new keys, upgrading existing keys, maintenance of existing keys, and deletion of old keys. The KMS must securely communicate with the CMS outlined above.

Registration process

All people accessing Australian Government health and social services benefits from 2010 will be required to have registered 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 release a discussion paper on the registration process for public comment in February 2007. 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 and homeless people.

Security and privacy

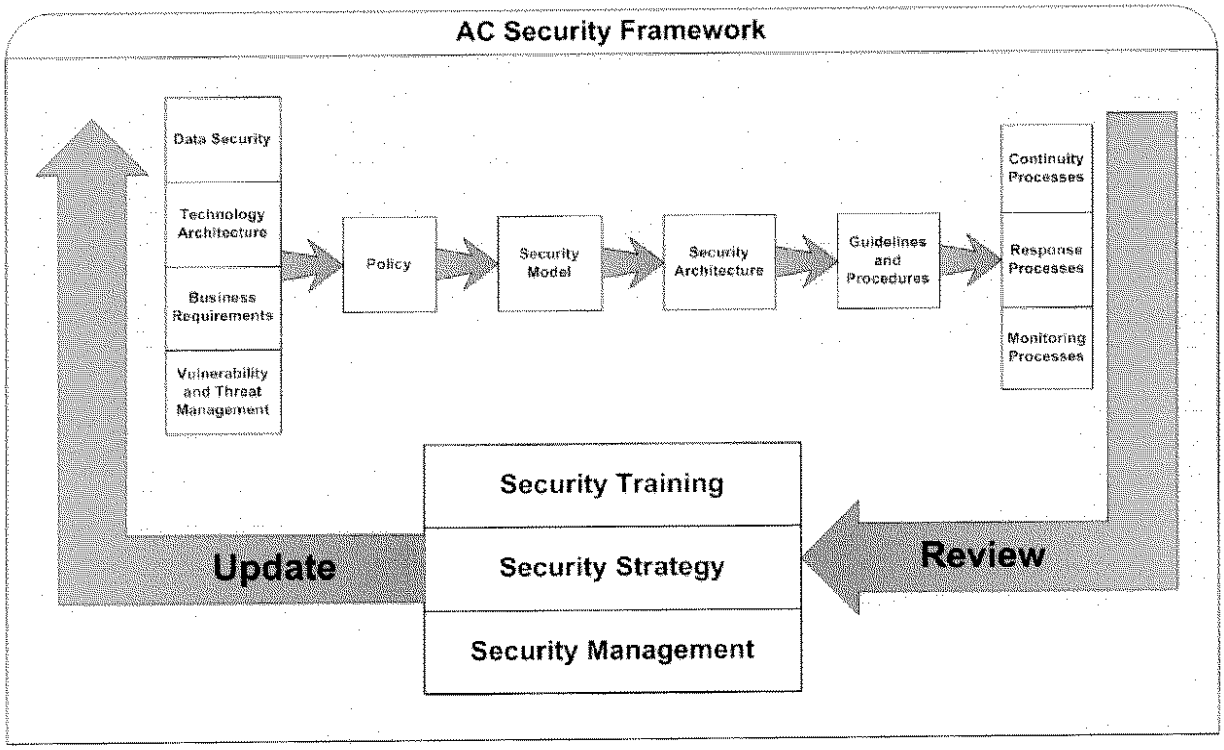
Protecting the security and privacy of individuals' information is paramount and the Government and the Department have put in place a range of measures to ensure that the legal and operational infrastructure underpinning the access card protects this information.

The Consumer and Privacy Taskforce chaired by Professor Allan Fels, AO recommended in its first report that a comprehensive legislative framework be developed for the access card program.

The Government supports the Taskforce's recommendation and this is reflected in the proposed legislation.

Privacy and Security Enhancing Architecture

DHS has made a significant commitment to ensuring that comprehensive security is engineered into every aspect of the program, from the initial conception through design, and the entire life of the program.

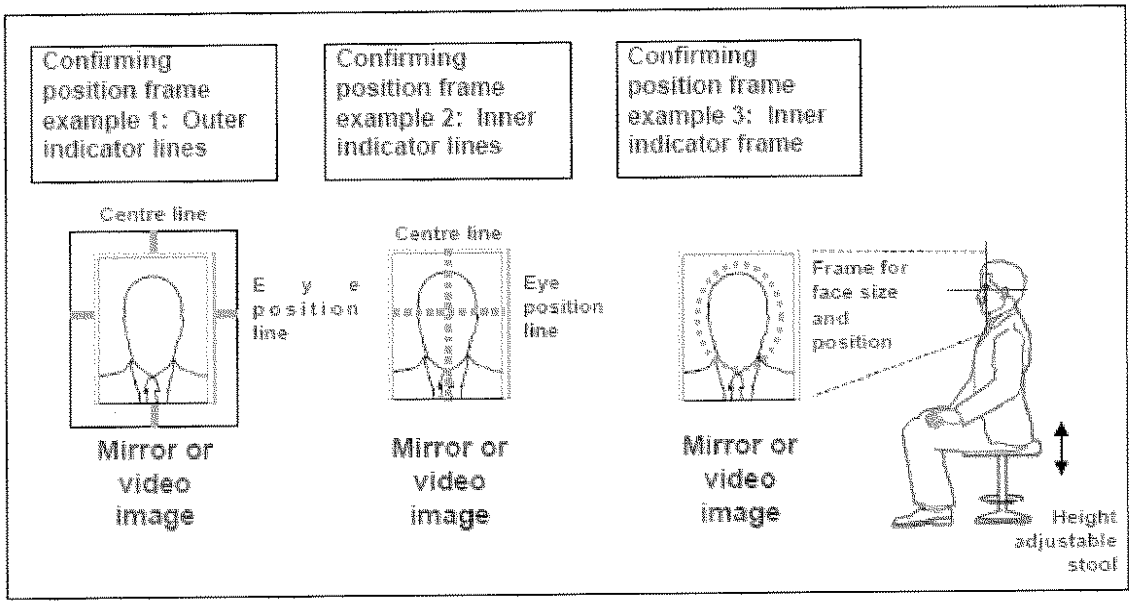


The ACS will use advanced and proven smartcard security technologies. This will be a significant improvement on the outdated magnetic strip and cardboard cards in use today.

Security is built into the chip and onto the card to prevent and detect tampering with the physical card, and to secure the cardholder'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 driver's licence. Importantly, the cardholder's photograph will be on the surface of the card. Swapping, borrowing or stealing cards will be far less attractive for those attempting to access benefits they are not eligible to, as a 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 that there will be 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

Physical security on the card will involve 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, for example, by a high quality Optical Variable Device.

Information in the chip in the card will be protected using advanced technology such as encryption, PIN protection and secure zones. It can only be accessed via authorised personnel, using authorised readers.

Restricting access to 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 DSD. 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 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 those parts of the ACS being delivered by the contractor.

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 and personalisation 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 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 cardholder. 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 ACS 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 ACS, 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 Card Issuance and Management 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 draft 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.

The following table provides an overview of these measures.

	Event	Department's rights and remedies under the Draft Card Issuance and Management Agreement
1.	The contractor: - 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.	The contractor is required to indemnify the Department for any resulting claims. The contractor's liability for damages is unlimited. The Department will be able to call on the financial guarantee. The Department will have remedies against the contractor's parent under the parent company guarantee. 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. The Department may also have the right to terminate the agreement and exercise rights of step-in. 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).
2.	The contractor fails to meet a service level or key performance indicator.	The Department may be entitled to claim service credits attributable to that failure. The Department will have the right to claim an appropriate level of damages.
3.	The contractor is late in meeting a milestone, other than due to an event out of the control of the contractor.	The contractor must provide reports indicating the nature and extent of the delay and the work-arounds that it is to implement. 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. The Department will have remedies against the contractor's parent

		under the parent company guarantee. 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. 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. 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).
4.	The contractor otherwise breaches the agreement.	The Department will have the right to claim an appropriate level of damages. The Department will be able to call on the financial guarantee. The Department may have remedies against the contractor's parent under the parent company guarantee. 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. The Department may have the right to terminate the agreement and exercise rights of step-in. 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).
5.	The contractor becomes insolvent or ceases, or threatens to cease, to conduct business.	The Department will be able to call on the financial guarantee. The Department will have remedies against the contractor's parent under the parent company guarantee. 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. The Department can order cards, chips or card issuance services directly from any of the approved subcontractors. The Department will have the right to terminate the agreement and exercise rights of step-in. 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).
6.	Contractor walks away from the project.	The Department can bring a claim against the contractor for default under, and repudiation of, the agreement. The contractor's liability is unlimited. The Department will be able to call on the financial guarantee. The Department will have remedies against the contractor's parent under the parent company guarantee. 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. The Department will also be entitled to exercise a right of step-in and to terminate the agreement. 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).

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 DHS;
- 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

DHS 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 program including for back-up and security purposes.

Timetable

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

Event (indicative only)	Proposed Date
Issue of RFT	31 January 2007
Closing time for RFT	5 p.m. 14 March 2007 (local Canberra time)
Presentations and site visits (if required)	To be determined
Notification to preferred tenderer(s)	End April 2007
Negotiation of draft agreement	June 2007
Signing of agreement	Mid June 2007
Design phase complete	July 2007
Development phase complete	October 2007
Australian Government security evaluation commences	End November 2007
System testing complete	December 2007
Australian Government security evaluation complete	February 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 program, consultation with a range of groups is continuing.

The next two procurement processes will involve tenders for Transaction Delivery Providers and IT Infrastructure. It is expected that these will be released during the second quarter of 2007.

The Consumer and Privacy Taskforce will release its discussion paper on registration for public comment in February 2007. This will be available through the access card website – www.accesscard.gov.au.