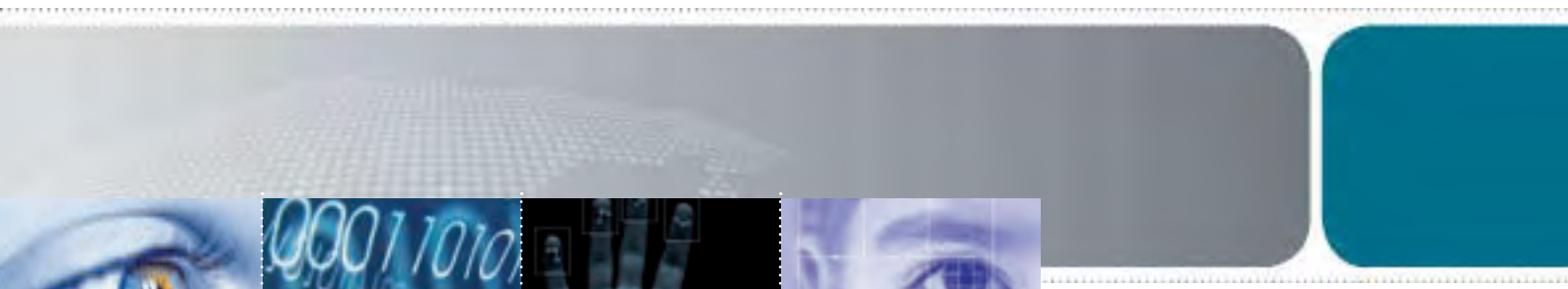




Australian Government  
Department of Immigration  
and Citizenship

# Identity Matters

Strategic Plan for Identity Management in DIAC **2007-2010**



---

# Contents

---

	Identity Matters	1
01	Plan purpose	4
02	Plan ownership	5
03	Intended audience	5
04	Operating environment	6
	The external environment	6
	• Global movement	6
	• Terrorism	7
	• Growth in identity crime	8
	• Faster processing and the use of biometrics to anchor identity	8
	The internal environment	9
	• Third party processing of clients	9
	• Electronic processing of clients	9
	• Refugee and humanitarian entrants	10
	• Palmer and Comrie reports and recommendations	10
	• Systems for People	11
	Background to the current identity management strategy	12
	Industry partners	13
	An Integrated Strategy Model for Identity	13
05	Key definitions associated with identity	15
	Identity	15
	Identity crime	16
	Identity management	16
	Biometric technology put simply	16
	Biometrics in DIAC	17

06	Identity management in DIAC	18
	The vision	18
	The goals	18
	Key deliverables	18
	• Organisational change	19
	• Identity services capability	19
	• Identity resolution capability	20
	• Biometrics at the Border	21
	Identity management processes	22
	• Collecting better identity data from our clients	23
	• Verifying identity data against existing information held in DIAC's or other agencies' systems	23
	• Managing identity data	24
	• Resolving identity	24
	• Sharing identity data with other agencies that have a legitimate need to know	26
07	National Identity Security Strategy	27
	DIAC's role in the NISS	27
08	International identity strategies	28
	Global Document Examination Network	29
09	Governance and reporting	30
10	Key benefits of DIAC's identity management strategy	31
11	Major milestones during 2007-2010	32
12	Description of the vision at 2010	33
	Organisational change	33

	Identity services capability	34
	Identity resolution capability	34
	Biometrics at the Border	35
13	Critical success factors	36
	Organisational change	36
	Identity services capability	36
	Identity resolution capability	37
	Biometrics at the Border	37
	Appendix A to Identity Matters, Roadmap 2007–2010	39
	Roadmap April - June 2007	40-41
	Roadmap July - September 2007	42-43
	Roadmap October - December 2007	44-45
	Roadmap January - March 2008	46-47
	Roadmap April - June 2008	48-49
	Roadmap July - September 2008	50-51
	Roadmap October - December 2008	52-53
	Roadmap January - March 2009	54-55
	Roadmap April - June 2009	56-57
	Roadmap July - September 2009	58-59
	Roadmap October - December 2009	60-61
	Roadmap January - March 2010	62-63
	Roadmap April - June 2010	64-65
	Notes	66



## 01: Plan purpose

This strategic plan represents a statement of the vision for the management of client identity as an integrated DIAC business function. It articulates the business need for identity management, the external and internal operating environment, the business impacts and potential benefits for the Australian Government and society as well as the business ownership, governance arrangements and key elements of the identity management strategy. It focusses on the prevention and reduction of identity fraud within DIAC programmes.

DIAC contributes to a whole-of-government approach to managing identity and preventing identity fraud by: establishing the identity of persons applying for entry to Australia or for other immigration related services or citizenship; verifying identity at the border; and establishing a consistent foundation identity for non-citizens to use in the Australian community, from initial contact through to when they become Australian citizens.

The *Strategic Plan for Identity Management in DIAC 2007-2010* focusses on the implementation of identity management as part of the *Systems for People* business transformation process. It covers all DIAC business functions with the aim of delivering an assessed, verified, consolidated and consistent single view of a client identity.

It is a three year plan, covering the period 2007 to 2010. While DIAC has been working on matters of identity since 2002-03, the identity management strategy, and the supporting biometric capabilities and tools, are still being developed and progressively deployed – there remains much to do before a mature and fully integrated identity management capability is delivered.

This plan addresses the strategy for the overarching implementation of identity management across the department's functions, of which Biometrics at the Border is a key element. The role of DIAC as the lead agency, in partnership with the Department of Foreign Affairs and Trade (DFAT), the Australian Customs Service (Customs) and the Office of the Privacy Commissioner (OPC), in implementing biometric technologies to enhance border security is covered in more detail in the *Strategic Plan for Biometrics at the Border 2005-2010*.



## 02: Plan ownership

Identity Branch has ownership of The *Strategic Plan for Identity Management in DIAC 2007-2010*. On behalf of the department, and in consultation with business areas, Identity Branch is responsible for:

- facilitating, guiding and monitoring the implementation of identity management across the department's business
- researching, testing and developing the required supporting biometric tools
- providing a range of ongoing identity management services
- developing an identity resolution capability.

Identity Branch also has responsibility for managing and reporting on DIAC's contribution to whole-of-government identity initiatives, particularly the Biometrics at the Border capability and the National Identity Security Strategy, as well as the development of processes and technologies that are compatible with Australia's key international partners.

## 03: Intended audience

This plan is intended for use by the DIAC executive and DIAC business areas, as well as by key stakeholders and external agencies that have a role in managing identity. It provides an important context document for DIAC staff, many of whom will be required to implement the strategy and to access and use the identity management tools.



## 04: Operating environment

1. A number of external and internal environmental factors are driving the need for a well-planned, effectively coordinated and comprehensive identity management strategy in DIAC. One of the challenges for the evolving strategy and its implementation is to keep pace with identity-related developments occurring within DIAC, nationally and internationally, as well as in the biometric tools and the supporting system solutions.
2. The DIAC approach to identity management must:
  - cater for all pertinent DIAC business functions
  - achieve a balance between identity risk and business efficiency
  - form part of the *Systems for People* programme of business transformation and system changes
  - provide for the continual exploration of innovations in identity management and the accompanying technology
  - contribute to the national identity strategy
  - be compatible with developments in international identity management and the deployment of biometrics in Australia's key trading partners.
3. The strategy is to be implemented in a time of considerable change, in both the external and internal environment, for the purpose of helping to combat one of the fastest growing crimes of the twenty-first century—identity fraud.
4. We live in a time of global trade and the ever-increasing movement of people around the world, on either a temporary or a permanent basis. Australia continues to have one of the largest migration programmes, and in 2005-06 accepted some 143 000 new permanent residents as well as hundreds of thousands more as temporary residents for business, study or working holiday purposes. As a major tourist destination, millions of tourists also crossed our borders. During the year, DIAC facilitated over 23 million movements of people into and out of the country.
5. One of the fundamental principles of the movement of people is that nations have the sovereign right to determine who enters their borders.

### The external environment

#### Global movement



By extension, nations also have the sovereign right to grant entry only to those they have approved for entry, and not to any substitute or false identities. Identity does matter. Unfortunately, there are many reasons why some people might seek to conceal their true identity, such as previous rejection for permanent or temporary entry, criminal associations or backgrounds, or national security reasons. There are also those who change their identity for legitimate purposes, who inadvertently create multiple or alternative identities in our systems.

6. The identity of those entering our country has importance extending well beyond security at the border. Some 43 per cent of Australia's population were either born overseas or were born to parents who were migrants. In 2005-06 the department conferred citizenship on 103 350 new citizens.
7. While there is no evidence of systemic identity fraud in our migration programmes, there are identified risks in some of our procedures. It is important that we clearly ascertain the identity of those who enter the country, many of whom will remain to form part of the fabric of our rich and culturally diverse Australian society.

There are also a number of external factors that have given impetus to the need for the Australian Government and DIAC to implement an identity management strategy.

### Terrorism

8. The events on and following 11 September 2001 placed increasing attention on the management and security of borders. *The 9/11 Commission* report states, '*the challenge for national security in an age of terrorism is to prevent the very few people who may pose overwhelming risks from entering or remaining [in a country]*'.
9. The report further states, '*For terrorists, travel documents are as important as weapons. Fraud in identification documents is no longer just a problem of theft... A fundamental problem ...is the lack of standardized information in "feeder" documents used in identifying individuals.*'
10. Given the capacity of terrorist groups for establishing ' sleeper cells ' in a target society, it is imperative that such people are detected at the entry point or, failing that, are not able to alter their identities to suit their planning purposes.

## 04: Operating environment

### Growth in identity crime

11. Advances in technology have enabled international and domestic organised crime syndicates to perpetrate identity theft and fraud on an unprecedented scale, to the extent that identity fraud is now recognised as a major organisational, economic and security risk for the future.
12. The alarming increase in identity fraud or theft as one of the fastest growing crimes, expanding from personal identity theft to include corporate identity theft, is well recognised. Identity related crimes cost countries such as Australia, the United Kingdom and the United States of America billions of dollars each year. As well as crimes for individual financial gain, there are clear links between identity related crimes and money laundering or the funding of terrorism activities.
13. In this context, public and private sector agencies in many countries are focusing on proof-of-identity (POI) documentation and the undisputed need to effectively establish and verify the identity of people in order to minimise the creation of false or multiple identities.
14. On a more specific immigration theme, people smuggling and human trafficking remain major issues where the falsification of identities and documents plays a part.

### Faster processing and the use of biometrics to anchor identity

15. Globally, the increase in the use of international air travel is placing pressure on governments, airlines and airport owners and border processing agencies. One of the challenges for DIAC is to implement adequate measures to verify the identity of non-citizens who travel to our country while continuing to use technology innovations to enhance the efficiency of travel for our residents and citizens.
16. Australia, like the United States of America, United Kingdom, New Zealand, Canada and many other countries, has developed an e-passport and is investing in the further development of biometric technology to improve identity verification in a broad number of situations, including border processing.

## The internal environment

### Third party processing of clients

17. Australia has streamlined the way it processes applications in a number of ways, including the introduction of electronic processing and the use of independent third parties. DIAC staff no longer directly interview the majority of those who seek to come to Australia. Instead, many applicants are interviewed by third parties, such as migration agents in the case of applications for longer term residence, student agents or travel agents for shorter term entry. Clients' applications are completed and the accompanying documentation is gathered before being passed to DIAC for decision. In 2005-06 there were 3163 registered migration agents.
18. Other third parties assist with specific phases in the processing of visa applications, for example:
  - Health Services Australia and doctors overseas conduct medical examinations and assessments on behalf of the department.
  - Recognised international providers conduct International English Language Testing System (IELTS) examinations to determine whether applicants can demonstrate functional English language ability for some visa categories, such as the general skilled migration stream or international students.

19. The involvement of multiple and third parties in visa processing opens up avenues for identity fraud as a number of people handle the case and see applicants at the various stages. It is important that applicants present in person for medical or language tests and do not send a substitute identity.

### Electronic processing of clients

20. In order to sustain ever faster processing despite increasing numbers of people movements, DIAC has implemented a number of world class systems, including the Electronic Travel Authority and the Advanced Passenger Processing system. Under these systems clients can apply for a visa via a third party, or online, and an electronic visa is issued. The take-up rate of online applications continues to grow. Identity controls need to be designed to meet the specific challenges of electronic processing. These identity checks must work in tandem with the controls built in to these systems and without affecting the efficiencies gained. As DIAC further streamlines processes to progressively obviate the need for visa labels in passports, this provides an added incentive to implement electronic means to verify the identity of clients.

## 04: Operating environment

### Refugee and humanitarian entrants

21. Refugee and humanitarian clients bring their own challenges. In addition to increasing numbers of applicants, many do not possess any proof-of-identity documentation and the majority are displaced to outside their country of origin. It is often difficult for DIAC staff to effectively establish the identity of these applicants. The size of the humanitarian programme is set at 13 000 places each year. In 2005-06 some 80 000 people applied under this programme to enter Australia from overseas.

### Palmer and Comrie reports and recommendations

22. The need to clearly establish identity and to ensure a consistent identity is sustained was highlighted during 2005, when two inquiry reports were released that made recommendations in relation to how DIAC manages the identity of its clients. These were the *Inquiry into the Circumstances of the Immigration Detention of Cornelia Rau*, known as the Palmer Report<sup>1</sup>, and the *Inquiry into the Circumstances of the Vivian Alvarez Matter*<sup>2</sup>, known as the Comrie Report.

23. Ms Cornelia Rau, a permanent resident, and Ms Vivian Alvarez, an Australian citizen, were inadvertently detained as potential unlawful non-citizens. In examining the circumstances surrounding these two cases, both inquiries found limitations in the department's ability to accurately identify its clients and to match or correlate variations in client records. The Palmer Report in particular made a series of recommendations encompassing the establishment of an Immigration Status and Identity Group and changes to the way the department captures and records client identity.
24. The Ombudsman's Office has also released a number of reports into immigration cases that make recommendations in relation to client and identity management.
25. A key priority for DIAC during 2006 was the more rapid development of revised business processes and the supporting biometric capability to accurately identify people taken into immigration detention to ensure that citizens and lawful non-citizens are not detained. In the longer term, the establishment of a single client identity for all DIAC clients should help to prevent the recurrence of such incidents because there should be only one DIAC record with any name changes or variations effectively linked.

1 Inquiry into the Circumstances of the Immigration Detention of Cornelia Rau, Mick Palmer AO APM, Commonwealth of Australia, July 2005.

2 Inquiry into the Circumstances of the Vivian Alvarez Matter, Office of the Commonwealth Ombudsman Report No. 03/2005, September 2005.

## Systems for People

26. In February 2006, the department reviewed its major systems and client processing functions and the recommendations arising from these reviews informed the *Systems for People* programme. Under *Systems for People*, the department is undergoing a comprehensive business transformation and its IT systems are being redesigned to deliver a better integrated suite of systems that will mitigate the issues raised by the various external reports as well as the DIAC reviews. A key aim of *Systems for People* is to allow staff to see a single, consolidated view of a client's record. The benefits are described in Figure 1.

27. The *Systems for People* programme will run over the period 2006-2010. In the 2006 Federal Budget, the government announced funding of \$495 million, over four years, for the programme. It will provide staff with the information and tools they need to do their job on their desktop, to the extent that staff can:

- see a single view of a client's history
- be confident about a client's identity
- be confident that they have a client's only record
- be confident that data is correct
- access all the required sets of screens tailored to their job role
- access the reports they need.

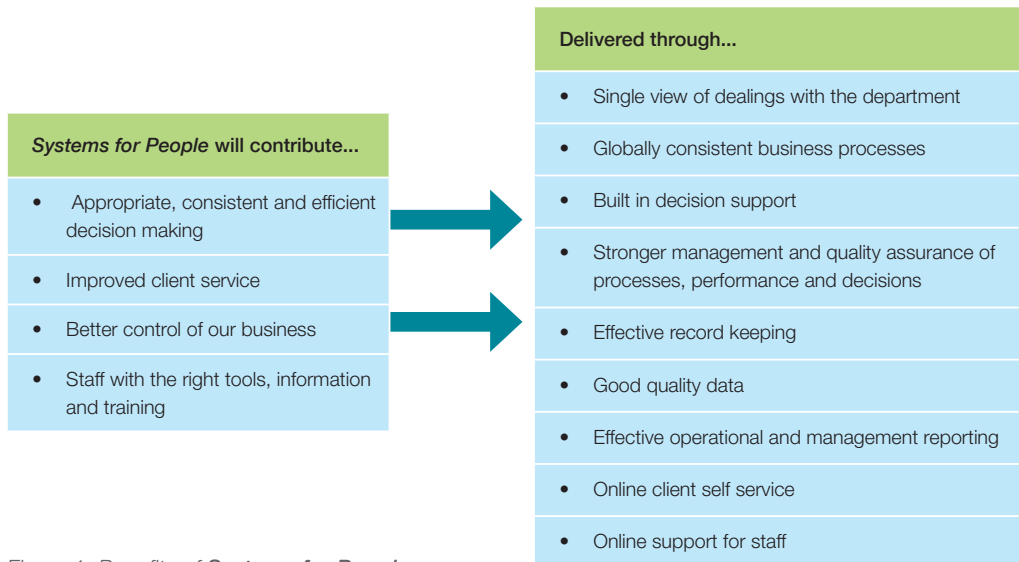


Figure 1: Benefits of *Systems for People*

## 04: Operating environment

28. All of these services will be provided in a single, usable system – available on every desktop through portal screens. As each portal is developed, the related business processes will be reviewed and required changes will be implemented at the same time as the portal release. Portals will be developed to cater for various uses, such as by client service staff and managers. External portals will be developed for client self-service, stakeholders, partners and contracted providers.
29. The identity management strategy is an important aspect of the DIAC business transformation process, and will assist in ensuring that DIAC staff can access a single view of a client – whose identity has been established and maintained.

### Background to the current identity management strategy

30. In January 2003, the department prepared a paper *Prevention and Management of Identity Fraud against DIMIA Programs*, which reported that: *'there is no evidence to suggest widespread identity fraud problems within any DIMIA programmes. However, there is ample anecdotal information to indicate that abuse is occurring on a regular basis, that it is complex, varied in nature and difficult to dismantle.'* This paper made 22 recommendations aimed at strengthening the department's ability to detect and deter identity fraud, and led to the establishment of Identity Branch.
31. Recognising that a multi-agency approach was required, DIAC, in conjunction with DFAT, Customs and the OPC, sought funding for a Biometrics at the Border initiative. In 2003-04 the agencies received funding for one year to research and pilot some of the proposed systems. When this was successful, the agencies received further funding in the 2004-05 budget of \$214 million over four years. The DIAC component is \$42.9 million over four years to develop biometric applications and to improve the identification and screening of non-citizens at the border. The implementation of Biometrics at the Border is due to be reviewed as part of the 2008-09 budget process.
32. In 2004 DIAC developed an identity management strategy and an identity roadmap based on the Biometrics at the Border initiative. The *Systems for People* programme and the Palmer, Comrie and Ombudsman reports resulted in unanticipated changes that have impacted on the Biometrics at the Border strategy in terms of approach, business integration, technical integration and schedule. This strategic plan has been developed to take account of these changes and to articulate the broader vision for identity management in DIAC.

33. The revised strategy for identity management in DIAC supports the three strategic themes for the department of:
- an open and accountable organisation (interactions with clients will be more readily traced through a single client view)
  - fair and reasonable dealings with clients (clients can expect a better service if their interactions with the department are recorded consistently)
  - well trained and supported staff (the consolidated client view assists staff in their work and supports better decision making).

### Industry partners

34. DIAC will deliver the identity management strategy through multiple industry partners. Unisys was selected to partner DIAC for three years, commencing late 2006, as the provider of a suite of suitable biometric solutions, software tools and a range of identity management services, including research. Identity Branch and Unisys must work in conjunction with IBM, DIAC's strategic partner for *Systems for People*.
35. If the identity management strategy is to succeed it is critical that the department makes best use of, and effectively integrates, the tools provided by Unisys and IBM. The new tools will also need to efficiently and effectively build on DIAC's existing identity management capability.

### An integrated strategy model for identity

36. The tiered model in Figure 2 illustrates how identity management will be realised via:
- strategy, architecture and innovation
  - a business model
  - identity services
  - the resultant identity product.
37. This is a fully integrated model, governed through business priorities and a programme/portfolio management approach. Its aim is to ensure a business driven approach to solutions for identity management within DIAC.
38. The first layer provides the business motivation for identity management, including the rationale, mission, vision, goals and objectives, strategies and tactics required. It incorporates strategic and policy directives and forms the basis for the next layer.
39. The second layer builds on the strategic layer through developing a business architecture future vision for identity management within DIAC. This layer provides valuable information for planning purposes by exposing the organisational change required and the resources and effort needed to implement the model. It sets the scope and context for developing supporting information and technical architectures of the *Systems for People* programme for identity management.

# 04: Operating environment

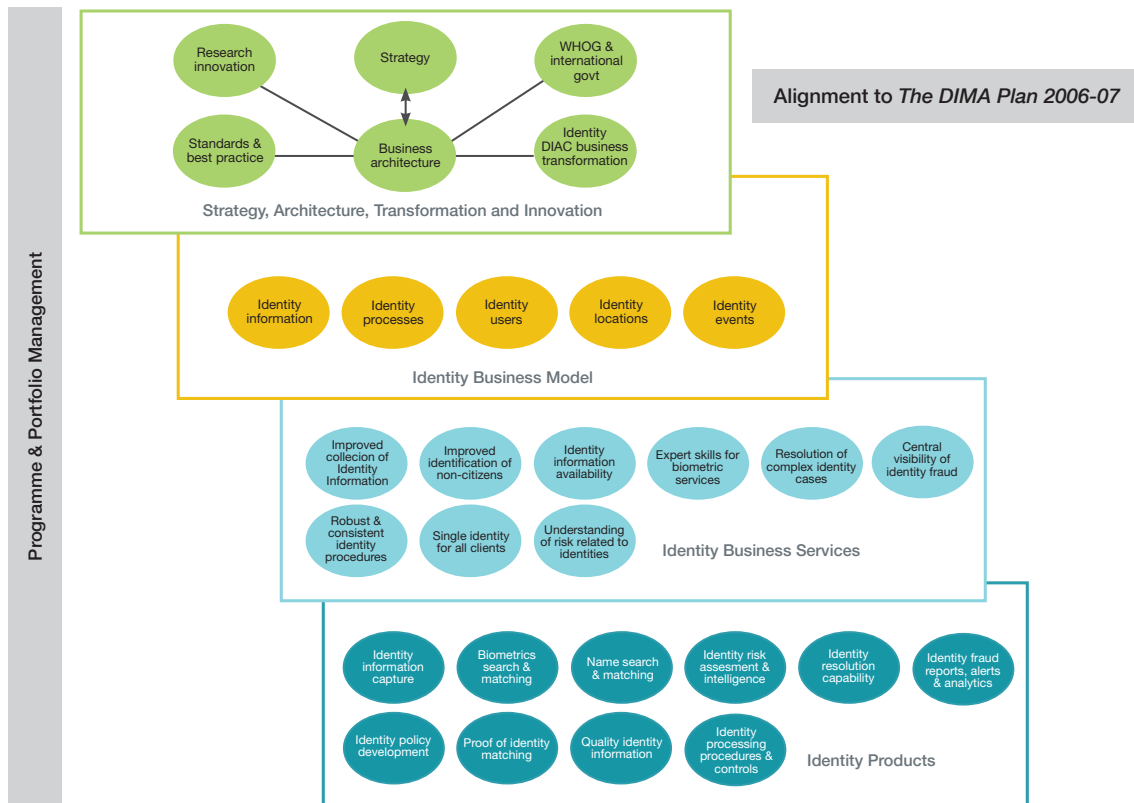


Figure 2: Integrated Strategy Model for Identity

- 40. The third layer represents the value derived from identity management and the benefits it will bring to DIAC officers, clients and the *Systems for People* programme.
- 41. The final layer represents the identity products which will be delivered. They are aligned to the value propositions as well as information, processes, events, people and locations via the business architecture and they represent a full product suite – which, when delivered, implements the identity strategy.

## 05: Key definitions associated with identity

42. To ensure the strategy is implemented cohesively it is important that those involved have a shared understanding of what is intended by the terms identity, identity crime, identity management and biometrics.

### Identity

43. The identity of a person may be defined by an associated set of biographical attributes such as name, address, date of birth, gender, nationality, family composition, occupation, sample signature and a description of the person's physical attributes. These biographical attributes are often supported by important documentary credentials such as a passport or visa, a driver's license, birth certificate, marriage or divorce certificates, citizenship certificates and, sometimes, proof of residential address documents such as utilities bills. Some countries also employ a national identity card.

44. It is widely recognised that a person might change their biographical details and that documents can be tampered with or forged. A key aspect of the international and national strategies to combat identity fraud is the introduction of biometric tools to 'anchor' identity.

45. The identity management strategy entails following three steps shown in Figure 3. It involves:

- Enhancing the department's capability to ascertain and verify our clients' *biographical* details – building on our current processes to allow for greater consistency.
- Increasing our capacity to verify the authenticity of *credentials* supplied as proof of identity and improving our ability to detect fraudulent or stolen documents.
- Building the capacity for the use of facial image and finger scan *biometrics* to 'anchor' identity in selected programmes or processing points according to risk.

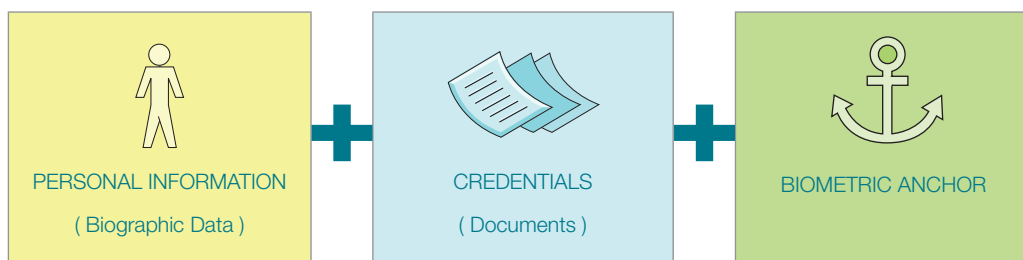


Figure 3: Establishing Identity

## 05: Key definitions associated with identity

### Identity crime

46. In 2006, the Australasian Centre for Policing Research stated '*Identity crime, which encompasses identity fraud and identity theft, is one of the fastest growing crimes and has been referred to as the "crime of the new millennium".*' False identities can be established in the following ways:

- creating a fictitious identity by manufacturing, forging or fraudulently obtaining legitimate documentation to satisfy proof of identity requirements
- altering one's own identity by making changes to name, date of birth or address
- stealing the identity of an actual person (living or dead) by using stolen personal information or fraudulently obtained, forged or stolen identity documents.

47. In an immigration context, identity fraud can be defined as<sup>3</sup>: *an individual representing him or herself as another person or as a fictitious person to obtain an immigration outcome.*

### Identity management

48. Identity management may be defined as an integrated system of business processes, policies and technologies that enable an agency to improve its:

- assurance that a person's identity claim is accurate

- ability to consistently record and view all information about a person's interaction with the agency – a single view of client
- ability to detect identity fraud or theft
- understanding of the risks related to false identity claims.

49. Identity management is most effective when the desired outcomes and benefits are clear. It must be supported by an integrated approach across an agency's programmes including policy, legislation and regulation, standards, business services, processes and procedures, training and guidance as well as the supporting computer systems and tools.

### Biometric technology put simply

50. Biometrics are measurable and consistent distinguishing features or behavioural traits that provide a means for recognising a person. There are different types of biometrics:

- Soft Biometrics, such as height, weight, and eye colour, provide information about a person, but lack the distinctiveness and permanence to sufficiently differentiate one individual from another.
- Stronger Biometrics, such as facial images, finger or iris scans and voice recognition, are unique to an individual and therefore provide a more reliable means for identifying a person. These biometrics can be captured and stored electronically and can often be measured and compared automatically (with manual verification of matches where deemed necessary).

<sup>3</sup> Prevention and Fraud Against DIMIA Programs, Border Control and Compliance Division, Canberra, January 2003, p 11.

51. A biometric template is a machine-encoded representation of the trait or characteristic created by a computer software algorithm. It enables comparisons to be performed to score the degree of confidence that separately recorded traits or characteristics identify (or do not identify) the same person.
52. A number of biometrics, such as facial image and finger scans, can be collected from a person and used in combination, depending on the business outcome required.

### Biometrics in DIAC

53. DIAC will use facial images as the primary biometric tool, in line with the approach of Customs, DFAT and some other international governments. Facial images are a mandatory biometric in ICAO<sup>4</sup> standard e-passports, whereas the use of finger or iris scans is optional. Finger scans will also be captured for some DIAC programmes where the identity risks are perceived to be greater. Initially this will include refugee and humanitarian entrants, onshore protection visa applicants and persons held in immigration detention centres.

54. In the future, finger scans could be used to check applicants for certain caseloads against biometric watch lists or to detect identity fraud. The identity management strategy envisages the use of finger scans for checking against DIAC, national, and eventually international biometric alert lists to detect whether or not a person presenting is a known criminal or terrorist. As DIAC's biometric holdings grow in size, finger scans will become an increasingly useful tool for detecting identity fraud.
55. DIAC's systems are being built with the capacity to accommodate the collection and use of multiple biometrics and combinations of biometrics. It is important that we build agile and scalable systems that are able to deal with advances in the technology and changes in our business requirements.
56. Resource and practical constraints mean that DIAC must manage identity on the basis of the perceived risk to its various programmes as well as the potential downstream consequences. There is no 'one size fits all' business process and biometric solution and the best-fit case will be sought, in consultation with the relevant business areas.

4 International Civil Aviation Organization