an
identity assurance framework
for government

December 2008

an identity assurance framework for government

December 2008

table of contents

the framework

1 Introduction

This Identity Assurance Framework outlines a structured approach to the coordination of identity assurance activity across government. Through promoting stronger leadership and coordination of identity assurance interventions, the Framework will provide greater assurance to the Government and the public that identity information is being managed appropriately and effectively within government, while maintaining privacy.

A number of effective identity assurance interventions are already in place in New Zealand, both across government and at the individual agency level. The Working Group responsible for development of this Framework found that any existing fragmentation of interventions could be addressed successfully by a more coordinated approach. The State Services Commission-led review of identity management across government, underway at the time of writing, is expected to confirm the findings about fragmentation and broaden the context for coordination to include wider identity management concerns.

New Zealand's approach to identity assurance is currently characterised by a focus on maintaining the privacy of individuals, while providing an acceptable level of security. There has been an emphasis on containing costs and ensuring that service access and usage is easy for customers. The nature of current identity assurance interventions reflects the historic perspective New Zealanders have had about personal identity information protection and national security.

This Framework identifies priorities for future action and establishes mechanisms for monitoring and reporting on progress. Over time, the interventions within the Framework will make a strong contribution to reducing vulnerabilities and building a seamless approach to identity assurance across government. In particular, greater use of authoritative sources of identity information by agencies when establishing the identity of their customers is required. It is expected this will contribute greatly to agencies' ability to better manage the risks associated with identity crime.

Better coordination of identity assurance interventions will also contribute to improved customer service and lead to better investment by government in identity-related systems and processes. The approach laid out in this Framework explicitly supports a number of Development Goals for the State Services.

Over time, this Framework will be reviewed and updated to ensure that it continues to meet the identity assurance needs of both the Government and the people it serves.

1.1 Development of the Framework

This Framework has been developed by an inter-agency working group reporting to a Chief Executive Reference Group chaired by the Chief Executive of the Department of Internal Affairs. This Framework is based upon content from a detailed report *(Secure Identities: Identity Assurance – A Cross-Government Response)* produced by the Working Group and finalised on 29 June 2007.

Government agencies represented on the Working Group are as follows: Department of Internal Affairs; Department of Labour; Inland Revenue; the New Zealand Transport Agency (formerly Land Transport New Zealand); Ministry of Social Development; New Zealand Police; the State Services Commission; and the Office of the Privacy Commission (as an observer). In addition, interviews were conducted with the following government agencies not represented on the Working Group that also have an interest in identity assurance: Ministry of Health; Ministry of Education; Ministry of Justice; the Accident Compensation Corporation; and the New Zealand Customs Service.

Consultation with government agencies on a draft version of this Framework was completed in late 2007.

2 Context

2.1 Defining identity assurance

This Framework focuses on identity assurance[1] within government. Identity assurance is about ensuring that business processes, procedures and systems are in place across government that provide assurance to both the Government and the public that identity information is being managed appropriately and efficiently[2]. In particular, this will involve assurance being provided that:

- appropriate privacy protections are in place for identity processes;

- people can establish and later verify their identity with government agencies with reasonable ease;

- agencies have appropriate processes in place for the secure management of the collection, storage, use and disposal of identity information;

- access to entitlements is not unduly affected, and where possible, will be enhanced through government identity-related interventions;

- identity crime is being prevented, as much as possible, from occurring; and

- identity information about individuals is managed consistently across government to ensure individuals do not use false or fictitious identities; and

- effective and coordinated investment in identity assurance systems is happening across government.

Alongside the above, agencies also need to ensure customer convenience wherever possible and a commitment to 'putting right' any mistakes made about individuals in relation to identity assurance.

2.2 The roles of government agencies in identity assurance

Many State sector agencies have a direct interest in identity assurance issues. An agency's involvement in identity assurance generally falls within one or more of the following activities:

- providing an authoritative source of identity information;

- undertaking an activity where the collection and management of identity information plays an important role in the agency's core business; and/or

- developing, overseeing, investigating or enforcing aspects of identity assurance as part of the agency's policy and legislative context.

This Framework applies to State sector agencies that fall into one or more of the these categories.

While identity information may be held in more than one place within government, there are several authoritative sources of identity information in New Zealand:

- the Department of Internal Affairs (DIA) is the authoritative source for most New Zealand citizens and also holds authoritative identity information for many non-New Zealand citizens (for example, marriage, death and name change information);

- the Department of Labour (DOL) is the authoritative source for non-New Zealand citizens who visit or reside in New Zealand; and

- other agencies also act as authoritative sources for some categories of identity information. For example, New Zealand Customs Service (Customs) hold information on the identity of Australian citizens visiting New Zealand that is not held by either DIA or DOL, and Inland Revenue (IR) holds information on the identity of offshore non-citizens liable to pay New Zealand taxes.

Other agencies use identity information, and produce documents/records that are often accepted as evidence of identity (for example, driver licences issued by the New Zealand Transport Agency, New Zealand citizenship through DIA).

Customs plays an important role at the border and is responsible for processing over 9 million air passengers' movement across the border that requires each passenger to be identified and recorded.

---

1   The term 'identity management' is not used as that term is commonly defined more widely than the scope of this Framework.

2   It is important to note that identity assurance is not used here in an absolute sense. Rather, this Framework is based on the notion that assurance will always relate to levels of confidence.

The State Services Commission (SSC) has a number of roles in relation to identity. These roles include that SSC is a central agency, has the Office of the Government Chief Information Officer, leads the All-of-government Authentication Programme, and is currently conducting a review of identity management across government.

DIA has two key identity assurance roles that support government:

- ensuring New Zealand's approach to identity is trusted and well led; and

- 'kaitiaki' (trusted custodian) of New Zealanders' authoritative identity information.

The first of these roles relates to DIA's leadership in strategy, policy, services and standards for identity information. Once implemented, this Framework will provide an important mechanism for DIA to assure the Government and the public that identity information is being managed appropriately and effectively within government. The second role relates, in particular, to the authoritative identity information held by DIA (containing information on births, deaths, marriages, civil unions, passports and citizenship).

3 Challenges, the solution and outcomes sought

3.1 Challenges to be addressed by the Framework

While there are many effective identity assurance activities occurring both across government and at an individual agency level, there is an opportunity for agencies to manage identity assurance processes more effectively and in a more coordinated manner. There are a number of challenges this Framework seeks to address:

- **Building confidence in agencies' identity-related business processes, procedures and systems** – If one agency does not manage identity information well, this may compromise the operations of other agencies that rely on that agency's identity information and/or documents. As a result, agencies that lack confidence in, for example, the evidence of identity, back office data management and staff training processes of other agencies, will be driven to strengthen their own processes and/or accept a greater level of identity-related risk.

- **Creating alignment between agencies' business processes, systems and data** – Government agencies are not yet using identity-related standards consistently across the sector, and data is being collected and used in different ways. In addition, there is only limited use of data validation against authoritative identity information sources. Increased validation will enable government to better leverage its investment in authoritative sources.

  Recent cases have demonstrated the need to improve the alignment of business processes, systems and data in order to reduce vulnerabilities that could lead to identity crime, whilst providing efficient, privacy-enhancing access to identity information (e.g. through provision of customer-centric verification services).

- **Reducing fragmented investment in identity assurance** – The current 'fragmented' approach to identity assurance across government results in greater overall costs to government, and a lack of interoperable processes and systems between agencies.

- **Minimising identity crime** – Applying a best practice approach to identity assurance across government will better enable the government to mitigate the risks associated with identity crime.

There are direct risks and costs to individuals, resulting from the criminal misuse of identity information; as well as collective risks and costs that occur as a result of successfully executed identity crimes. Furthermore, these risks can even occur as a consequence of, or in spite of, interventions employed to prevent identity crime. Examples include situations where agencies' interventions are not comprehensive enough, or where an agency closes one loophole in its identity assurance processes and fraud is then perpetrated through another loophole.

The risks relating to identity can impact on numerous areas, including the public's trust in government, reputation (of individuals, agencies, and New Zealand), public safety, and individual and Crown finances.

3.2 Solution – An 'all of government' strategic approach

The solution to the challenges identified is an all of government strategic Framework which will provide assurance to the Government and the public that identity is being managed appropriately and effectively within government, while maintaining privacy.

A cross-government coordinated approach to identity assurance will enable:

- a consistent approach to collecting and using identity information – this will facilitate transactions between individuals and government agencies, and improves customer experience;

- agencies to develop interoperable processes and solutions cost effectively – interoperable processes will enable agencies to rely confidently on other agencies' prior processes, and reduce duplicate investment; and

- identity crime to be reduced through the sharing of information, intelligence, experience and knowledge between agencies.

If government agencies are effective at enhancing identity assurance, numerous benefits will accrue to the Government, and people in New Zealand generally. These include that:

- access to government services are provided to people who are who they claim to be;

- agencies identify and create opportunities for efficiencies, particularly through the use of 'build once and use many times' systems and/or process solutions;

- identity assurance approaches are privacy friendly (for example, individuals are only required to provide the types and amounts of evidence, or confirmation of their identity, that is appropriate to the types of services being sought);

- public trust in government is enhanced through the public having confidence that:

  - their privacy is protected;

  - government consistently applies good practice standards to the management of individuals' identity information; and

- the risks posed by identity crime are mitigated effectively, thereby reducing the downstream impacts that identity crime can have on agency programmes, national security and the community.

3.3 Outcomes

The Identity Assurance Framework will contribute to the following outcomes for government:

Governance – Identity information is well managed, ensuring New Zealand's approach to identity is trusted and well led. This will provide assurance to Government and New Zealanders that value for the money is being achieved from investments made in the management of identity information.

Protection – New Zealanders are protected from identity crime. People are better protected from the consequences of the misuse of their identity information through effective management of the information, consistent with their reasonable expectations for privacy and civil liberties.

Facilitation – Reliable and accessible identity assurance processes facilitate transactions between individuals and government agencies. People can easily, efficiently and cost-effectively access services to which they are entitled, that have an identity assurance component.

3.4 Contribution to the State Sector Development Goals

Implementation of this Framework will make a significant contribution to achieving the Development Goals for the State Services.[3] This Framework will be reviewed regularly to ensure alignment with any future changes to the Development Goals.

In particular, this Framework will contribute to the Coordinated State Agencies goal by helping to ensure that government agencies are working together, sharing capabilities and using effective networks to enhance identity assurance.

This initiative will also contribute to the Development Goals of:

- Networked State Services – through the effective use of technology to enhance identity assurance within government;

- Accessible State Services – through good identity assurance activities that result in better customer service, including reducing barriers to accessing services in relation to the amount of identity information people provide to agencies;

- Trusted State Services – through Government and the public having assurance that identity information is being managed appropriately; and

- Value-for-Money State Services – through coordinated identity assurance activity across government, so that efficiencies and economies of scale can be achieved.

---

3   The Development Goals for the State Services can be found at: http://www.ssc.govt.nz/development-goals

4 An Identity Assurance Framework for Government

4.1 Scope of the Framework

The Framework applies to agencies within the New Zealand State sector that require confidence in the identity of people they deal with, and other agencies that have an interest in identity assurance.

The scope for this Framework includes identity assurance as it relates to the identification of individuals rather than businesses. However, as government agencies have regular interactions with companies that they need to identify, government agencies may choose to apply relevant aspects of this Framework in that setting.

The Framework addresses identity assurance issues both in the domestic and international contexts. This is important as a number of New Zealand State sector agencies have a significant international component to their work, including providing services to overseas-born people. The international aspect of the work carried out by many agencies has a direct impact on the Government's ability to manage identity effectively onshore. For example, DOL has identified that there is a high level of identity-related risk associated with verifying the identities of non-New Zealanders in the visa issuance process. Managing identity risk in immigration is critical to managing national security and criminal risks to New Zealand.

The extension of services developed for the State sector to the private sector is an issue that will need to be considered as services are developed. The Framework does not cover the way that the private sector manages identity information. However, If State sector agencies manage identity more effectively, this could have positive downstream benefits for private sector organisations which rely on government-issued identity documents and processes.

4.2 Principles underpinning the Framework

The following principles[4] underpin the Identity Assurance Framework.[5]

Acceptability – Ensuring that the identity assurance approach is generally acceptable and accessible, taking into account the different needs of people, and avoids creating barriers. High standards of customer service are maintained.

Privacy and security – Suitable protection must be provided for information owned by both people and the Crown. People's privacy must be appropriately protected, by adherence to the twelve information privacy principles.[6]

All-of-government coordination – Balancing the public's and agencies' concerns about independence with the benefits of standardisation across government. Ensuring that government agencies share information appropriately in order to: prevent, detect and investigate the misuse and abuse of identity; facilitate transactions between government and individuals; and reduce costs where possible.

Customer convenience – Wherever possible, customer convenience will be considered an important aspect in the design of agency identity assurance processes and systems.

Endurance and adaptability – Ensuring systems, processes and procedures are enduring, yet sufficiently flexible to accommodate a wide range of current and future needs.

Value for money – Ensuring the recommended approach is affordable, reliable and efficient for the public and government agencies.

Technology interoperability – Ensuring that where appropriate, identity assurance systems are separate while also being interoperable.

Risk-based approach – Providing a risk-based approach whereby the level of identity assurance interventions carried out by agencies is in direct proportion to the level of identity-related risk associated with that agency's functions.

Legal compliance – Identity assurance systems must comply with relevant law, including privacy and human rights law.

Incremental and consultative approach – New systems, processes and procedures should be implemented in increments, following extensive piloting and consultation.

---

4 The principles are based on the following: deliberations of the Working Group; the Privacy Act 1993; the Policy and Implementation principles for electronic authentication of individuals carrying out online transactions with government agencies, agreed by Cabinet in 2002; and the *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age* by Ann Cavoukian, Information and Privacy Commissioner of Ontario.

5 In some cases compliance with international standards may influence how these principles are adopted.

6 Privacy Act 1993, section 6.

5 Future (target) state for identity assurance

This section outlines the desired future state that will provide the Government and the public with assurance that identity information is being managed effectively across the State sector.

5.1 Overview

The desired future state is characterised by:

- strong leadership and governance relating to cross-government secure management of identity assurance systems and processes;

- the establishment of agency centres of expertise in identity assurance, to enable:

  - ongoing identification of identity issues facing government;

  - an identity assurance capability for New Zealand and non-New Zealand identities;

  - a more coordinated approach to governance and funding of identity assurance initiatives; and

  - greater access to expertise and leadership on identity-related issues within government;

- smarter, more secure and more efficient use of government's authoritative identity information;

- where possible, identity information will be stored only once, at source agencies with greater use of electronic checking by other agencies against the authoritative identity information source;

- standardisation of how agencies collect and manage identity information;

- appropriate technologies being implemented that enable more effective identity assurance;

- full integration of identity-related risk management approaches into agency processes and systems, and more effective use of tactical intelligence sharing across government;

- robust and continuous availability of identity services to New Zealand and New Zealanders;

- agencies have the people, capability and culture to facilitate good identity assurance practices;

- the appropriate legislative framework is in place to facilitate good collaborative identity assurance practices; and

- increased public awareness about how to protect against identity theft and crime (i.e. what to do and when), and what to expect of government agencies in relation to identity assurance.

5.2 Description of future (target) state by transformation categories

The future state described in the following sections has been built around the following seven 'transformation categories':

- Leadership and governance
- Standardised identity information management
- Appropriate data collection and management
- Technology as an enabler
- People, capability and culture
- Legislative framework
- Public awareness.

A category approach was taken to this Framework in direct response to the type of issues under consideration. Any successful identity assurance initiative at the cross-government level requires a comprehensive approach, which recognises that many factors contribute to overall identity assurance. For example, if the approach does not include leadership and governance, and people, capability and culture considerations, then investments in technology may not achieve their desired benefits. For this reason, through attention to each of the categories listed above, implementation of this Framework will more likely result in government having 'all its bases covered' regarding identity assurance.

5.2.1 Interventions to achieve future state

A range of interventions will be required to move government toward the desired future state. A number of proposed interventions, as well as some that are already underway, have been identified and described in Part Two of this Framework.

While these interventions have been organised into relevant transformation categories, they are largely inter-related. Changes in one category may impact on the others, and many of them depend on the successful implementation of interventions from other categories for their own success. With commitment from across government the desired future state can largely be achieved by 2015, in step with the State Services Development Goals.

5.2.2 Transformation category 1: Leadership and governance

> **Current state:**
>
> - some agencies are already providing leadership and/or expertise for certain aspects of identity assurance.
>
> **Future state:**
>
> - an Identity Assurance all-of-government, coordinated approach, led by DIA, is fully established and operating within government, with effective governance and funding arrangements in place; and
>
> - agencies are using a common identity fraud control framework to detect and prevent fraud and to manage fraud cases after they have occurred.

A collaborative approach will be implemented to manage cross-government issues relating to identity assurance. This collaborative approach will include formal centres of identity assurance leadership and expertise. This model will be similar to approaches to managing other cross-government interests within government.

Key outcomes that this cross-agency approach will help to achieve are:

- a formal avenue for gaining expertise on identity assurance issues facing government (for example, through an ongoing identity assurance governance group or forum).[7] This avenue will provide assurance that identity issues are being proactively recognised and managed within government on an ongoing basis;

- collaborative decisions within government about developments and investments. For example, more 'build once and use many times' solutions being developed;

- the relevant thought leadership and/or expertise roles within government will be formally recognised and government's expectations of these 'leaders' identified. Key roles include those relating to authoritative identity information (DOL and DIA), developments in identity management (State Services Commission), the detection and prevention of identity crime (New Zealand Police), and guardianship of the handling of personal information (Office of the Privacy Commissioner);

- ongoing research, monitoring and evaluation of cross-government identity assurance initiatives and developments;

- greater coordination of identity initiatives – for example, the Cross Government Biometrics Group will ensure a managed approach to the implementation of biometric technology across government, including areas such as interoperability and cost-effectiveness; and

- more effective application of resources across government to prevent and detect identity fraud, based on a common identity fraud control framework.[8]

---

7 The Working Group process demonstrated the usefulness of convening agencies with a core interest in identity assurance, on a fairly regular basis, to discuss issues and determine future interventions for dealing with these issues.

8 The Identity Fraud Control Framework will provide guidance for agencies on preventing and detecting identity fraud, and managing fraud cases after they have occured.

5.2.3 Transformation category 2: Standardised identity information management

> **Current state:**
>
> - custodian agencies are encouraging and supporting the use of existing standards that relate to identity information[9]; and
>
> - some agencies are implementing existing standards.
>
> **Future state:**
>
> - high data quality, appropriate interoperability and a standardised approach across all of government; and
>
> - data and systems are protected and made available only to authorised parties.

A cultural shift will have occurred in government that will see agencies applying a consistent and coordinated approach to their identity assurance interventions, where possible. It will be necessary to identify appropriate identity assurance standards for relevant agencies.

While a number of standards already exist for government (e.g. relating to online authentication and data), there are other areas which require future work (e.g. regarding biometric technologies).

Agencies will be responsible for recognising the effect that their decisions have on other agencies, for example, where an agency issues a document or credential that is later used by other agencies as evidence of identity[10]. In these cases, agencies that issue documents/records used to establish identity, and agencies that use these documents, will work together (and with DIA) to identify the implications/risks of these documents being used as evidence of identity.

A second and related cultural shift will be that agencies will determine, when issuing documents, the specific identifying information that needs to be included. For example, where a document with a photograph has a particular purpose that is not identity-related, the document may not need to include a name or date of birth information. The photo alone may be enough to identify a particular individual for a given purpose.[11]

---

9   For example, the Authentication standards.

10 Numerous documents and data sources issued within government are later used by other agencies as evidence of a person's 'social footprint', within an overall identity establishment process.

11 When determining identifying information that needs to be included on government-issued cards, agencies will also need to take into account any secondary uses of the card which are legislated, (for example, if the card is also able to be used to prove a person's age).

5.2.4 Transformation category 3: Appropriate data collection and management

Current state:

- most agencies are cleansing their data and removing duplicate records;

- some agencies are using documents verified at source;

- some agencies are matching data with other agencies; and

- the Police Identity Intelligence Unit is collecting data, but involvement by other agencies is limited.

Future state:

- greater use of online verification, with minimal identity-related information held by service agencies and less reliance on the use of physical documents; and

- agencies will accept that an identity once verified by the authoritative source of the identity information will be accepted subsequently without further verification, or minimal verification steps being required.

In future, government will be much smarter and more efficient in the use of authoritative identity information sources. Between them, DOL and DIA hold authoritative identity information about New Zealand's long-term residents and citizens. This identity information is, and will continue to be, the result of rigorous identity establishment processes. Robust data management will give assurance that identity information is always available and failover systems are in place should identity information or systems be inaccessible.

Traditionally, agencies have relied largely on documents to identify individuals. The future state sees a significant reduction in the use of documents, with a corresponding increase in efficient data validation. Document or data validation services provide assurance that the data in a paper document or application form provided by the individual is not counterfeit or fictitious. However, these services will not provide assurance that the individual is the legitimate 'owner' of that identity information.

Agencies may carry out increased automated checks in the back office to validate identity data, while ensuring that people do not experience undue delays.

In some cases, agencies will receive identity information from the individual concerned, and verify that information with the authoritative identity information source. As such, the individual is aware of the information collected, and consents to the verification of that information.

A key element of this future state is reliance on "just-in-time" verification through real-time access to authoritative identity information, either on a record-by-record basis, or groups of records (for example, the passenger manifest of an air or marine vessel for the purposes of border control).

5.2.5 Transformation category 4: Technology as an enabler

Current state:

- some agencies are developing identity data validation services;

- some agencies are using biometric data matching, risk profiling and data mining;

- some agencies are contributing to international systems for managing identity at the border; and

- the Government Logon Service and the Identity Verification Service are being deployed to enable the public to transact securely with government.

Future state:

- technologies will enable more effective identity assurance, increased security, while maintaining privacy across government;

- agencies will be consistently using Government Shared Services in conjunction with their business specific applications; and

- biometric technologies will be integrated into identity-related processes where appropriate, and in a cost-effective manner.

Full-scale identity verification services that provide assurance of a person's identity will eventually become the norm, where verification is necessary as part of establishing entitlement. Authoritative identity information sources in government will be accessed through real-time online access with appropriate authorisation. The Identity Verification Service (IVS) will be the first of these services, and will allow people to establish their identity, to a high level of confidence, to agencies online and in real-time. This is an opt-in service.

Two key aspects of the future services that will operate in government are:

- the citizen-centred nature of these services – the IVS, for example, will enable individuals to authorise the release of specific identity information about them; and

- agencies will have reduced the amount of identity information they hold about their customers – through the use of real-time verification processes against authoritative identity information sources.[12]

Two primary benefits from this approach relate to government efficiencies and fraud prevention. Centralised validation and identity verification services will enable agencies to rely on other agencies' identity information to reduce their costs and avoid duplication. Secondly, by significantly reducing the number of paper documents agencies require, this not only provides customers with easier access to government services, it also prevents agencies from accepting counterfeit documents.

The above approach to accessing authoritative identity information sources relies heavily on having very high standards of data accuracy and security, and is reliant on progress in Transformation categories 2 and 3. The future state will see a high degree of standardisation being applied to how agencies collect and manage identity information. This in turn will ensure that:

- the quality and interoperability of data will be greatly enhanced;

- individuals are not being unduly prevented from accessing services or deterred from meeting obligations, and that their privacy is not being unduly impeded; and

- risks are being mitigated effectively across government (i.e. if all agencies are using standardised approaches to identity-related risk mitigation).

The future state will also see identity-related fraud control approaches fully integrated into agency processes and systems. This will contribute to enhancing operational effectiveness by increasing the level of assurance surrounding identity related practices. It will enable better decision-making, improve the quality of operations and contribute to better delivery of identity related services to the public.

---

12 Identity information in this scenario does not need to be held by the agency accessing that data (unless there are other valid business reasons for doing so). Rather, real-time validation or verification against source data is carried out and the result, rather than the data, is then recorded by the receiving agency.

A risk management approach will include:

- greater levels of automated risk profiling and intelligence-driven systems, which provide opportunities for enhanced customer services, as the bulk of applications for services can be handled with greater speed and efficiency;

- enhanced opportunities to detect and prevent crime[13]; and

- appropriate use of technology, which may include biometric technology.

At the macro level, intelligence exchange within government will be improved. In particular, agencies will have greater commitment to, and better use of, the New Zealand Police Identity Protection Register. Greater sharing of agency watch lists is another mechanism that may become business as usual in the future.

5.2.6 Transformation category 5: People, capability and culture

Current state:

- most agencies are monitoring developments in this area, and seeking to raise awareness;

- some agencies capture information about, and report, identity crime; and

- some agencies have developed and enforce staff integrity policies.

Future state:

- wide-spread understanding and demonstration, by State servants across government, of best practice and the risks associated with managing identity information.

A strategic approach to managing identity information needs to be well led. A widespread understanding of security needs and good practices, in relation to designing, implementing and monitoring systems and processes, is required across government. Agencies need to understand any risks associated with managing identity information and have the skills, expertise and knowledge available to develop and implement appropriate mitigation strategies.

State servants (and private sector staff working on behalf of State sector organisations) will understand the risks associated with managing identity information and demonstrate best practice.

---

13 For example, the use of more intelligent systems will enable staff to focus more on 'riskier' cases and specialise in fraud detection and prevention.

5.2.7 Transformation category 6: Legislative framework

> **Current state:**
>
> - there is on-going review and amendment of some legislation in relation to identity assurance by individual agencies.
>
> **Future State:**
>
> - a comprehensive legislative approach that enables successful prevention, detection and deterrence of identity crime, balanced with appropriate levels of privacy protection, freedom of information, operational efficiency and excellent customer service.

In order for a strategic approach to identity assurance to be successful, legislation needs to support cross-agency efforts to implement and manage quality identity assurance systems and processes. It is imperative therefore, that any legislative barriers to effective identity assurance practices are identified as soon as possible and effective mitigation actions are taken. This is particularly important where existing legislation prevents effective law enforcement collaboration. Any review of the current legislative approach will require significant input from both a wide range of government agencies and consultation with the public.

5.2.8 Transformation category 7: Public awareness

> **Current state:**
>
> - some agencies are providing guidance to the public about how to protect their identity.
>
> **Future State:**
>
> - a high level of public awareness of their role in protecting their own identity information, and their expectations of the State sector in managing that information.

A cultural shift is required in relation to public awareness. This relates to both what the public can do to assist in preventing identity theft and fraud, and also to what the public can expect of government agencies in relation to identity assurance. A common understanding of the rights of customers will be achieved within the State sector, and will be promoted equally alongside communications about the public's responsibilities. Government also needs to ensure that the public has an adequate understanding of the technologies and processes that are used to manage identity assurance. Agencies will need to coordinate their communications to have maximum impact.

6 Glossary of terms

For the purposes of this Framework, the definitions outlined below apply.

All-of-government Authentication Programme – A programme of work to develop, operate and maintain all-of-government standards and services related to online authentication. The Authentication Programme is led by the State Services Commission.

Authentication – The process of establishing, to the required level of confidence, the identity of one or more parties to a transaction. Consists of identity establishment and ongoing confirmation.

Authoritative identity information[14] – Identity information that can be relied upon across government for most administrative purposes. For any given identity attribute, the government often has one agency that has the best capability of collecting, verifying, maintaining and asserting that attribute.

Biometric information – Physical characteristic of a person (e.g. iris, face, gait, voice).

Biometric recognition – The process of matching an input biometric to stored biometric information. In particular, biometric recognition refers to comparing the biometric input from an individual to the stored biometric template about that individual (for example, face images, fingerprint images). Also includes one-to-many biometric matching programmes.

Biometric technology – Technology used to manage and use biometric information.

Counterfeit document – A document that has been entirely manufactured to look as though it is a genuine document.

Civil liberties – Fundamental individual rights, such as freedom of speech and religion, protected by law against unwarranted government or other interference.

Data Validation Services – Web-based services that can validate the authenticity of the data on a named individual's identity document/s, or the data provided by the individual, to approved organisations. (the New Zealand Transport Agency currently operates one of these services in relation to the driver licence. DIA are developing a data validation service, which will validate passport and birth data to authorised users in the near future).

Evidence of identity – The types of evidence that, when combined, provide agencies with confidence that an individual is who they claim to be (for example, a passport and a birth certificate).

Government Logon Service – An all-of-government shared service that provides ongoing re-confirmation of online identity to participating agencies to the desired level of confidence.

Identity[15] – A person's 'identity' is their unique self and so each person has one and only one identity.

Identity assurance – Refer to section 2.1.

Identity attributes – Identity attributes describe a person's identity and these attributes constitute 'identity information'[16].

Examples of identity attributes include name, address, and age; unique identifiers such as GST number, NHI number, and driver licence number; biometrics such as fingerprints and facial geometry; and 'reputational' or aggregated information such as health, educational and criminal records.

Identity crime – A broad term used to describe the misuse and abuse of identity, including identity fraud and the impersonation of an individual (which is sometimes referred to as 'identity theft'). Identity crime can underpin and facilitate a range of other criminal activity.

Identity information – Information that describes a person's identity.

---

14 Definition taken from *Identity Management Review: Report on Progress*, POL (08) 165, 30 June 2008.

15 Definition taken from *Identity Management Review: Report on Progress*, POL (08) 165, 30 June 2008.

16 Definition taken from *Identity Management Review: Report on Progress*, POL (08) 165, 30 June 2008.

Identity management[17] – The gathering, verification, storage, use and disposal of identity information.

Identity-related risk – Any risk for a particular service that results from an individual's identity being incorrectly attributed.

Identity Protection Register – A register, administered by the New Zealand Police, which collects identity crime intelligence for use as both an investigative and measurement tool.

Identity Verification Service – A proposed all-of-government shared service that provides individuals with the option to verify their identity authoritatively, online, and in real-time with participating agencies to a passport-level of confidence.

Information matching – The comparison of identity data by public sector agencies, for the purpose of producing or verifying information about an identifiable individual. Information matching takes place pursuant to legislative authority and subject to an information matching agreement, governed by the Privacy Act.

Social footprint evidence – Evidence that an individual uses their claimed identity in the community (for example, this may include evidence such as driver licences and Inland Revenue numbers).

---

17 Definition taken from *Identity Management Review: Report on Progress*, POL (08) 165, 30 June 2008.

implementing the framework

7 Introduction

Achievement of the future state set out in the Identity Assurance Framework will require the coordinated implementation of a range of interventions by agencies. The future state described is targeted to be achieved over the next 5–10 years. This timeline is necessary as a number of interventions involve the development of new shared services that will require agency uptake and/or involve the passage of legislation.

Part Two sets out:

- Interventions that will contribute to achieving the future state (refer to section 8);

- Summary of key work programmes that will lead to significant transformation of identity assurance across government (refer to section 9);

- Governance arrangements to ensure ongoing implementation and development of this Framework (refer to section 10); and

- Monitoring and reporting arrangements that will support the implementation of this Framework (refer to section 11).

8 Interventions

A comprehensive set of organised interventions is required to implement the Identity Assurance Framework and to transform the way government agencies currently manage identity information and identity-related processes.

The following sections set out interventions required for each transformation category. Key points to note when reading these sections:

- Interventions have been classified as being immediate (within the next two years) or medium-term (over the next 5–10 years) interventions;

- Medium-term interventions should be considered as indicative only at this stage, except where these are otherwise mandated (for example, through e-GIF). A review of the immediate interventions in approximately 12 months will help confirm, and update if necessary, the medium term interventions;

- Some interventions will contribute to more than one transformation category, however, each intervention has been only categorised by a single transformation category to avoid repetition;

- Agencies responsible for implementing specific interventions are identified;

- Where the term "border agencies" is used this is reference to agencies with responsibilities at the border, and includes some or all of the following agencies: DOL, Customs, Ministry of Agriculture and Forestry, New Zealand Food Safety Authority, Aviation Security Service, Maritime New Zealand, and DIA; and

- Where the term "all relevant agencies" is used, this refers to those in the New Zealand State sector that require confidence in the identities of people they deal with. Agencies will determine for themselves whether the interventions that require "relevant agencies" to implement them are relevant to them and this decision will be based on the functions they undertake and whether identity-related risk has any bearing on these functions.

8.1 Transformation category 1: Leadership and governance

The following interventions are required to achieve the future state for the **Leadership and governance** transformation category.

Immediate interventions:		Agency / agencies
Intervention 1a:	Agencies to establish communities of practice for government in identity-related fields, including:	
	• Prevention and detection of identity crime (through Identity Intelligence Unit)	NZ Police
	• Biometrics (including identification of preferred biometrics for NZ government and development of Standards).	DIA
Intervention 1b:	Cross-government identity assurance Community of Practice established (refer to section 10 for details).	DIA
Intervention 1c:	Development of a Monitoring and Reporting Plan for identity assurance interventions designed and completion of a snapshot of current status of identity assurance interventions (refer to section 11 for details).	DIA
Medium-term interventions:		
Intervention 1d:	DIA and DOL to take increased leadership role as custodians of key government identity information. This will include managing the identity information in a way that allows appropriate access by other agencies while also protecting data quality, and the privacy of individuals.	DOL & DIA
Intervention 1e:	Development of an Identity Fraud Control Framework[18], in order that agencies can make informed decisions about where their own and government's collective fraud prevention, detection and enforcement resources should be focussed for maximum impact.	DIA

---

18 The Identity Fraud Control Framework will be guidance material that assists agencies to determine what they can do to better prevent and detect fraud. For example, it will provide an outline of the types of interventions that reduce certain types of fraud. Development of the Identity Fraud Control Framework will involve subject matter experts from various agencies.

8.2 Transformation category 2: Standardised identity information management

The following interventions are required to achieve the future state for the **Standardised identity information management** transformation category.

Immediate interventions:		Agency / agencies
Intervention 2a:	Identification by agencies that issue documents/records (that are used by other agencies to establish or verify identity) of any weak links in their business processes that may cause identity assurance issues for other agencies.	
	DIA, as part of its EOI Standard custodianship role, will advise agencies of any implications/risks arising from the above, and will update the EOI Standard as required.	All relevant agencies
Intervention 2b:	Review and updating (if required) of Authentication Standards following completion of agency pilots.	SSC & DIA
Medium-term interventions:		
Intervention 2c:	Implementation of the Authentication Standards within relevant agencies.	All relevant agencies
Intervention 2d:	Standards for the gathering, storage, use and disposal of biometric information to be developed and implemented by agencies (to be progressed as part of the Cross Government Biometrics Group's work programme).	DOL
Intervention 2e:	Ongoing identification of relevant data standards for government, to facilitate data sharing, and development or adoption where required.	DIA

8.3 Transformation category 3: Appropriate data collection and management

The following interventions are required to achieve the future state for the **Appropriate data collection and management** transformation category.

Immediate interventions:		Agency / agencies
Intervention 3a:	Analysis of how government can better leverage existing investment in authoritative identity information sources.	Agencies responsible for authoritative data / SSC
Intervention 3b:	Agencies to proactively review current data sharing and other back office processes to enhance fraud detection (e.g. through data mining capability, profiling and use of watch lists).	All relevant agencies
Intervention 3c:	Improvements to intelligence exchange within government to ensure relevant data (including biometric information) is being provided to the Police Intelligence Unit.	All relevant agencies
Medium-term interventions:		
Intervention 3d:	Implementation of identity & biometric components of the various planned border sector work programmes, including:	
	● Immigration Business Transformation (IBT) Programme	DOL
	● CusMod2	Customs
	● Passport Redevelopment Programme	DIA
	● Passport Data Access Project	DIA
Intervention 3e:	Implementation of real-time data sharing to support identity assurance processes at the border. This includes: Advanced Passenger Processing; Regional Movement and Alerts System; and exchange of data between NZ and Australian Customs.	All relevant agencies

8.4 Transformation category 4: Technology as an enabler

The following interventions are required to achieve the future state for the **Technology as an enabler** transformation category.

Immediate interventions:		Agency / agencies
Intervention 4a:	Pilot agency using Identity Verification Service (IVS) during 2008/09, with limited service available from 2009/10.	DIA & SSC with pilot agency
Intervention 4b:	DIA's Data Validation Service (DVS) piloted during 2008/09, with service available from 2009/10.	All relevant agencies
Intervention 4c:	Increased security features for key physical documents (including the Passport).	DIA
Medium-term interventions:		
Intervention 4d:	Intelligent risk-based processing built into key agency systems to enable targeting of greatest number of agency resources to riskiest cases, while enhancing customer services for the bulk of customers.	All relevant agencies
Intervention 4e:	Development of greater understanding across the government of the appropriate use of biometric recognition for identity assurance, including appropriately addressing privacy issues (to be progressed as part of the Cross Government Biometrics Group's work programme).	DIA
Intervention 4f:	Coordination of inter-agency system development at the border in relation to identity assurance and biometrics.	Border agencies
Intervention 4g:	Implementation of one-to-one and one-to-many biometric matching arrangements in agencies (where this is appropriate[19]).	All relevant agencies
Intervention 4h:	Full service IVS available as an opt-in service.	DIA[20]
Intervention 4i:	Full service DVS available to agencies.	DIA
Intervention 4j:	Introduction of real-time identity data validation services by agencies other than DIA (i.e. other holders of authoritative identity information).	All relevant agencies

---

19 Appropriateness will depend on, for example, whether privacy impact assessments have been carried out, whether sufficient oversight arrangements are in place, and whether sufficient safeguards are in place regarding false negative match results.

20 It is planned that the Government Technology Services will have moved from SSC to DIA by the time the full service IVS is available.

8.5 Transformation category 5: People, capability and culture

The following interventions are required to achieve the future state for the **People, capability and culture** transformation category.

Immediate interventions:		Agency / agencies
Intervention 5a:	Staff of agencies with identity related tasks to be trained on good practice identity assurance processes, and Privacy Act requirements. In addition, in-house experts in these areas to be identified.	All relevant agencies
Intervention 5b:	Operating procedures and internal documents should be updated to reflect required identity assurance capabilities.	All relevant agencies
Medium-term interventions:		
Intervention 5c:	Agencies to put in place ongoing staff integrity awareness training and controls to mitigate corruption risks and the risks associated with unauthorised/unjustified staff access to identity information.	All relevant agencies
Intervention 5d:	Agencies to ensure risk focus balanced with privacy considerations and excellent customer services.	All relevant agencies
Intervention 5e:	Increased agency input into the National Targeting Centre[21] to increase border security.	All relevant agencies

8.6 Transformation category 6: Legislative Framework

The following interventions are required to achieve the future state for the **Legislative Framework** transformation category.

Immediate interventions:		Agency / agencies
Intervention 6a:	Implementation of planned legislative changes, including:	
	• Births, Deaths, Marriages and Relationships Registration Amendment Act (to strengthen controls around access to increase individuals' awareness and control over how their information is disclosed);	DIA
	• Immigration Bill (addition of powers to introduce biometric-enabled identity processes for all people applying for a visa, protection and crossing the New Zealand border).	DOL
Medium-term interventions:		
Intervention 6b:	Drafting and passage of new legislation to enable the full Identity Verification Service.	DIA
Intervention 6c:	Review of the legislative framework within which agencies currently operate, in order to promote a consistent, enabling and enduring approach to managing identity components of legislation.	All relevant agencies[22]

---

21 Customs' National Targeting Centre provides targeting functions to support Customs' operations. It has three main areas of responsibility – passenger risk, trade risk and response briefing. It is a nexus between intelligence and operational delivery, enabling Customs' risk management priorities in both travel and trade to be operationalised through analysis and targeting. The Centre is increasingly being used to support other agencies' risk targeting activities. It liaises closely with a range of other agencies to advance inter-operability and improve capacity to respond rapidly and efficiently to a range of border threats. It currently has staff from the Ministry of Agriculture and Forestry, and Maritime New Zealand seconded to it. Further secondments from other agencies are anticipated.

22 While DIA can lead this work, it will require significant discussions and inputs from across government, including Ministry of Health, Ministry of Justice, the Office of the Privacy Commissioner and SSC. Further, public consultation will also form an important input to this process.

8.7 Transformation category 7: Public awareness

The following interventions are required to achieve the future state for the **Public awareness** transformation category.

Immediate interventions:		Agency / agencies
Intervention 7a:	Agencies to take steps to ensure that people are given appropriate information about when and why their identity information is being collected and/or shared.	All relevant agencies
Medium-term interventions:		
Intervention 7b:	Development of a public awareness strategy and implementation plan on how identity is protected, and how the public can assist.	DIA

9 Key work programmes

There are a number of work programmes being progressed within government that will lead to transformed identity assurance systems, among other things. A number of the interventions described in the preceding sections are being undertaken through these programmes.

Key programmes[23] of work already underway include, but are not limited to:

Programme	Agency responsible
All-of-Government Authentication Programme, including: • The Government Logon Service (GLS) • The Identity Verification Service (IVS)[24] • The Authentication Standards, including the Evidence of Identity Standard • Future Services work programme	 SSC / DIA
The Border Sector work programme (including Identity @ the border work stream)	Border agencies
Immigration Business Transformation programme	DOL
CusMod2	Customs
Ongoing management of the Identity Protection Register	NZ Police
Data Validation Service (DVS) development	DIA
Cross Government Biometrics Group	DIA
Proof of Identity Project	IR
Education Sector Authentication and Authorisation (ESAA)	Ministry of Education
Privacy, Authentication and Security (PAS) Project	Ministry of Health
Review of Identity Management Across Government	SSC

---

23 The SSC's Review of Identity Management Across Government will include a "list of current and planned identity management initiatives across the government" [POL (07) 430 refers].

24 The GLS and IVS are collectively referred to as 'igovt'. For further information refer to http://www.i.govt.nz.

10 Governance arrangements

To ensure the Identity Assurance Framework retains its relevance, new interventions must be supported by an action plan that establishes specific timelines, key milestones and agency responsibilities, including identifying lead agency responsibility. This will be an ongoing role for DIA.

Proposed arrangements for the implementation and ongoing management of the Framework are:

- A Chief Executive Group[25] will maintain an overview of progress towards meeting the future state outlined in this Framework. This Group will also support inter-agency collaboration.

- Monitoring and reporting on progress will be coordinated by DIA (refer to section 11). DIA will be responsible for reporting to Ministers and agencies (arrangements yet to be determined).

- A Government Identity Assurance Community of Practice, coordinated by DIA on an as required basis, will be used to share information, knowledge and experience between agencies as the Framework is implemented (existing inter-agency forums will be used if appropriate).

---

25 Governance arrangements, where possible, will align with those determined through the SSC's Review of Identity Management, underway at the time of writing.

11 Monitoring and reporting

The Framework will be supported by a Monitoring and Reporting Plan, to be approved by the Chief Executive Group, which establishes processes to:

- evaluate and monitor the implementation of the Identity Assurance Framework across government;

- facilitate an understanding of the extent to which the Identity Assurance Framework is achieving its stated outcomes; and

- report progress against the Framework.

The Monitoring and Reporting Plan will comprise of:

- a set of high-level key performance indicators and, where available, baseline data for each indicator; and

- a monitoring programme to measure progress over the life of the Framework.

The Monitoring and Reporting Plan will be complemented by the monitoring and evaluation of individual initiatives by the agencies responsible for implementing them.

11.1 Key performance indicators

A set of key performance indicators have been identified to provide a basis for determining progress towards achieving the outcomes of the Framework. The (initial) indicators[26] selected are as follow:

Establishment Phase Measures – These indicators will primarily be measures of the extent to which the Identity Assurance interventions are actually being implemented by agencies. They include:

- Agency uptake of IVS;

- Agency uptake of EOI Standard;

- Agency uptake of DVS;

- Agency participation in the NZ Identity Protection Register;

- Centres of expertise are established and recognised by other agencies;

- Staff training activities (as reported by agencies); and

- Regular reports are provided to Ministers and Chief Executives on progress with Identity Assurance Interventions (against Action Plan milestones).

Impact Measures – These indicators will focus on whether the Identity Assurance Framework is actually achieving the outcomes sought.

- Public/client awareness of identity assurance processes and initiatives;

- Client utilisation of IVS;

- Customer satisfaction with agencies' efforts to prevent identity crime;

- Numbers of privacy complaints related to identity assurance interventions;

- Average elapsed time between first known perpetration of identity crime and detection (NZ Identity Protection Register);

- Agency awareness and utilisation of the Identity Fraud Control Framework;

- Survey of participating agencies (e.g. to establish perceptions of levels of intelligence sharing etc);

- Agency administrative data (numbers of invalid credentials issued); and

- Agency administrative data (levels of "successful" identity crime using government documents or processes).

The above indicators will be measured by way of an annual survey of agencies with identity assurance responsibilities. In addition to the indicators identified, there is likely to be information (e.g. from one-off evaluations) that could provide useful contextual information to support the overall Monitoring and Reporting Plan. Further important data sources will emerge from work underway in individual agencies. There may also be other opportunities to further refine the set of indicators as future surveys and research and evaluation initiatives progress.

It will not be possible, in every case, to establish direct causal links between the Framework interventions and movements in the indicators. A range of other factors will influence each indicator. The value of this approach will be in looking at the indicators as a set, in the context of what we know about the impact of individual Framework interventions and external factors influencing the indicators, to inform an assessment of progress over time.

---

26 Indicators are not expected to be a static set, and will change over time with the addition of new interventions.