Hon Megan Woods, Minister for Government Digital Services

Hon Tracey Martin, Minister of Internal Affairs

Proactive Release Developing Options for a New Approach to Digital Identity Cabinet Paper

These documents have been proactively released.

5 November 2018, Cabinet Economic Development Committee Minute of Decision Developing Options for a New Approach to Digital Identity Cabinet Paper, Cabinet Office

5 November 2018, Developing Options for a New Approach to Digital Identity Cabinet Paper, Department of Internal Affairs

5 November 2018, Appendix A: Feasibility Study for a New Approach to Digital Identity, Department of Internal Affairs

Parts of this information release would not be appropriate to release and, if requested, would be withheld under the Official Information Act 1982 (the Act). Where this is the case, the relevant sections of the Act that would apply have been identified. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

Key to Redaction Codes:

- 9(2)(ba)(i) - protect information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied

- 9(2)(f)(iv) - maintain the constitutional conventions for the time being which protect the confidentiality of advice tendered by Ministers of the Crown and officials

- 9(2)(g)(i) - maintain the effective conduct of public affairs through the free and frank expression of opinions by or between or to Ministers of the Crown or members of an organisation or officers and employees of any department or organisation in the course of their duty

© Crown Copyright, Creative Commons Attribution 4.0 International (CC BY 4.0)
Developing Options for a New Approach to Digital Identity

Portfolios: Government Digital Services / Internal Affairs

On 31 October 2018, the Cabinet Economic Development Committee:

1. **noted** that:
   
   1.1 Budget 2017 established a tagged contingency of $7 million for the development of an alternative digital identity solution for New Zealand;
   
   1.2 funding of $1.85 million was drawn down in July 2017 to develop a business case for the transition to a digital identity marketplace;
   
   1.3 the Minister of Internal Affairs was invited to report back to Cabinet in December 2017 with a business case outlining the proposed transition and seeking drawdown of the remainder ($5.15 million) of the contingency [CAB-17-MIN-0185.13];

2. **noted** that officials have undertaken analysis across the New Zealand public and private sector landscape, and internationally, and have prepared the *Feasibility Study for a New Approach to Digital Identity* attached as Appendix A to the paper under DEV-18-SUB-0242 (using as much of the business case template as possible, given the iterative nature of the work);

3. **agreed** that in recognition of the emerging market in digital identity services, the government will continue working with citizens, agencies and the private sector to:
   
   3.1 develop options for a new approach to digital identity, including the long term role of government and the private sector in the provision of digital identity services;
   
   3.2 identify regulatory gaps;

4. **noted** that because there are sensitivities with how the government handles individuals’ personal data, the work programme will be guided by principles that place a heavy emphasis on:
   
   4.1 citizen consent and control;
   
   4.2 being customer centric;
   
   4.3 privacy and security by design;
   
   4.4 being open and transparent;
4.5 meeting broad stakeholder needs;
4.6 interoperability;

5 directed officials to prepare a detailed work programme that will include:
5.1 the development of a Digital Identity Trust Framework to establish leadership and set the standard for digital identity in New Zealand, and other policy work;
5.2 design and test worked examples;
5.3 engagement and transition (including implications for agencies);
5.4 governance and oversight arrangements;

6 agreed that the work programme will be approved and its delivery overseen by the Minister of Finance, Minister for Government Digital Services, Minister of Internal Affairs and Minister of Commerce and Consumer Affairs;

7 invited the Minister for Government Digital Services and the Minister of Internal Affairs to report back to the Cabinet Economic Development Committee by October 2020 on the outcomes of the work programme and any longer-term funding implications, and to report earlier as necessary to seek Cabinet decisions at key points to enable the work to progress;

**Financial implications**

9 rescinded the previous decision [CAB-17-MIN-0185.13] requiring a business case to release the remainder of the tagged contingency funding ($5.15 million); and instead

10 approved the following appropriations to meet the Department of Internal Affairs’ costs of continuing work to establish a digital identity ecosystem, with a corresponding impact on the operating balance:

<table>
<thead>
<tr>
<th>Vote Internal Affairs Minister of Internal Affairs</th>
<th>2018/19</th>
<th>2019/20</th>
<th>2020/21</th>
<th>2021/22</th>
<th>2022/23 &amp; Outyears</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Category Expenses and Capital Expenditure; Civic Information Services MCA Departmental Output Expense; Managing and Accessing Identity Information (funded by revenue Crown)</td>
<td>2.575</td>
<td>2.575</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

11 agreed that the changes to appropriations for 2018/19 in paragraph 10 above be included in the 2018/19 Supplementary Estimates and that, in the interim, the increases be met from Imprest Supply;
agreed that the expenses incurred under paragraph 10 above be a charge against the ‘Transition to a Digital Identity Marketplace’ tagged contingency, established as part of Budget 2017;

**Publicity**

noted that the Minister for Government Digital Services and the Minister of Internal Affairs intend to announce the digital identity work programme and seek the involvement of citizens and other stakeholders in its delivery.

Janine Harvey
Committee Secretary

**Present:**
Rt Hon Winston Peters
Hon Kelvin Davis
Hon Grant Robertson (Chair)
Hon Dr Megan Woods
Hon Nanaia Mahuta (part of item)
Hon Iain Lees-Galloway
Hon Jenny Salesa
Hon Damien O’Connor
Hon Shane Jones
Hon Kris Faafoi (part of item)
Hon Willie Jackson
Hon James Shaw

**Officials present from:**
Office of the Prime Minister
Officials Committee for DEV

**Hard-copy distribution:**
Minister for Government Digital Services
Minister of Internal Affairs

Proactively released by the Minister for Government Digital Services and the Minister of Internal Affairs.
Developing Options for a New Approach to Digital Identity

Proposal

1. Recognising the growing importance of digital identity and the emergence of a private sector market in digital identity products and services, this paper recommends that Cabinet direct officials to:

   1.1. continue working with citizens, agencies and the private sector to develop options for a new approach to digital identity, including the long term role of government and the private sector in the provision of digital identity services; and

   1.2. identify regulatory requirements.

2. Cabinet approval is sought to release the remainder of the contingency funding ($5.15 million) to enable officials to continue a programme of work over two years, overseen by relevant Ministers, with regular reports to Cabinet.

Executive summary

3. Identity is vital to everyday life. Being able to reliably prove who we are is a prerequisite for accessing and participating in society and accessing services, such as banking, voting, travelling, and healthcare. In a digital world, digital identity becomes more valuable and more complex as interactions and transactions no longer take place in person.

4. Trusted digital identity is a critical enabler of citizen and business participation in the digital economy and access to government services. Digital identity is a core component of the infrastructure needed to deliver the Government’s priorities on digital rights, digital inclusion and to grow the digital economy.

5. The government’s current suite of digital identity products, RealMe, was created several years ago in anticipation of the growing importance of digital identity and when there were no market alternatives. RealMe is highly secure and private.
6. However, on their own, RealMe services are not sufficient to meet current and future needs. RealMe has fallen short of projected usage by agencies and private sector organisations and has struggled to keep up with changes in expectations and requirements for citizens and businesses. In its current state, it is not flexible enough to provide the breadth of utility or simplicity of experience required.

7. Since the launch of RealMe, not only has the importance of digital identity grown but so has its complexity. Citizen and business online activity has increased, there have been and will continue to be developments in technology, and increased international connectivity.

8. An unregulated market for digital identity services has also emerged. Currently these services are inconsistent and disconnected, posing risks such as confusion, exclusion and inefficiency for both citizens and businesses. Identity service providers and organisations that rely on digital identity services, support government taking the lead in changing this environment.

9. There is an opportunity for government to take a leadership role in shaping the future direction of digital identity in New Zealand. We need to support development of the digital identity services market while protecting citizen interests, and identifying the future role of government (including RealMe) and the private sector. Maintaining the status quo will result in lost potential productivity for the economy, inefficient government and private sector investment, and a crowding out of the market through continued government subsidy of the limited RealMe services.

10. In line with other comparable jurisdictions, we consider that government will always have a role in this area. Currently, government is the main digital identity service provider. However, this may move over time to being a strong regulator as the market matures, and in response to citizens’ appetite for more convenient and interconnected services across the public and private sectors. We think that, given citizens’ high expectations about how government handles their personal data and increasing concerns about cyber security and privacy, this ongoing government role is vital to maintaining citizen trust.

11. Subject to Cabinet approval of the release of the remainder of the contingency funding, officials will deliver a work programme comprising three main work streams: Policy Development, Test and Design Worked Examples, and Engagement and Transition. The work programme will be delivered over two years, with regular reports and decisions brought to Cabinet at the direction of oversight Ministers, and culminating in a final report to Cabinet by October 2020.

12. This work will be undertaken in close collaboration with citizens, public agencies and the private sector. Officials will work with citizens to test possible new digital identity examples and to ensure that any options are customer-centred. Taking a more collaborative approach will allow government investment in digital identity services across the whole of the government system to be aligned and better utilised.
13. The approach will also foster innovation and investment from outside government to address the increasing complexity of citizen and organisation needs, and to respond to future changes. These benefits would only be realised once the Government has set an appropriate regulatory and policy framework (Digital Identity Trust Framework (DITF)).

14. How government addresses digital identity challenges is likely to be of interest to a wide range of stakeholders. We propose that the work is overseen by the Minister of Finance, Minister for Government Digital Services, Minister of Internal Affairs and Minister of Commerce and Consumer Affairs. We also recommend that an advisory group be established comprising senior officials from government agencies, the Privacy Commission and the private sector to ensure an independent and whole-of-system approach.

15. Recognising the sensitivity and risks associated with the proposed work programme and how the Government handles personal data, officials will be guided by the following principles:

<table>
<thead>
<tr>
<th>Customer-centric</th>
<th>better customer experience is a driver behind all options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and security by design</td>
<td>privacy, security and citizen control and consent ‘baked in’ from the beginning of the process</td>
</tr>
<tr>
<td>Open and transparent</td>
<td>wide consultation and co-design with citizens and other stakeholders; transparency of decision making</td>
</tr>
<tr>
<td>Meets broad stakeholder needs</td>
<td>balances the needs of a wide range of stakeholders</td>
</tr>
<tr>
<td>Interoperability</td>
<td>ensures interoperability with comparable jurisdictions</td>
</tr>
</tbody>
</table>

16. The proposed work will support the Government’s priorities to share New Zealand’s prosperity and to build a productive, sustainable and inclusive economy.

17. A business case was to be the trigger for the release of the remainder of the contingency funding. However, work to date has shown that a full business case, presenting a detailed and costed permanent solution to digital identity, is not appropriate or possible at this stage. The attached Feasibility Study (Appendix A) uses the business case template to the extent possible and outlines the detailed thinking to date and proposed direction of future work.

**Background**

18. Budget 2017 established a tagged contingency of $7 million for the development of an alternative digital identity approach for New Zealand [CAB-17-MIN-0185.13 refers].

19. Funding of $1.85 million was drawn down in July 2017, following the establishment of an independent transition team, to investigate and develop a business case for the transition to a digital identity marketplace.
Work to date

20. The independent transition team was established in July 2017, and hosted by the Department of Internal Affairs (DIA). The attached Feasibility Study (Appendix A) expands on the work done to date in the ‘discovery’ phase, which includes:

20.1 undertaking analysis of digital identity approaches across the New Zealand public and private sector landscape;
20.2 developing use cases to understand the user perspective;
20.3 leading Investment Logic Mapping exercises, workshops and forums to gain an in-depth understanding of agency and private sector needs and interests;
20.4 completing a high-level legislative and regulatory review;
20.5 researching Digital Identity Trust Frameworks in comparable jurisdictions (Australia, Canada and the United Kingdom);
20.6 researching approaches taken in comparable jurisdictions, including the role of government, and consulting directly with key players in Australia, Canada and the United Kingdom;
20.7 consulting widely with private sector organisations including parties relying on digital identity as well as providers of digital identity services; and
20.8 shaping the discussions and developments in several collaborative prototyping experiments and at the new industry-led Digital Identity NZ.

The Case for Change

Context

21. Identity is vital to everyday life. Being able to reliably prove who we are online is a prerequisite for accessing and participating in society and accessing services, such as banking, travelling, and healthcare. In a digital world, trusted digital identity becomes more valuable and more complex as interactions and transactions no longer take place in person.

22. A trusted digital identity is fundamental for people and organisations to engage safely and securely in the digital world. It allows for access to targeted services from government and other providers. It also enables businesses to realise the economic opportunities presented by an increasingly digital world. In sum, digital identity underpins accountability for every transaction in the digital world. Without a reliable, robust, and accepted digital identity, trust between entities cannot be sustained.
23. Government has invested in digital identity for the last 12 years because of its importance to citizens (to protect rights and support inclusion), the economy (to open up productivity and growth) and the delivery of government services (offering cost effectiveness). Government investment has been directly in services, primarily RealMe, and was introduced at a time when market alternatives did not exist.

24. The RealMe suite of services includes a single login for citizens to access government services, and a verified identity for citizens to prove who they are digitally. The RealMe Login is a “pseudonymous” username and password, while the RealMe Identity Verification Service (IVS) offers a high level of confidence in a person’s identity, packaged in a solution that emphasises privacy by design. RealMe IVS is available to both public agencies and the private sector.

25. The context for digital identity is explained more in the attached Feasibility Study.

**Digital identity today**

26. Since RealMe was launched, digital identity has become more important and globally connected:

26.1 Digital identity has become widely recognised as a critical enabler of digital activity. It is frequently cited as a high priority for enterprises and governments alike (examples of global research reports are included in the Feasibility Study). The Australian Federal Government in its 2018 budget, allocated A$92.4m on its digital identity programme;

26.2 The digital identity-related impacts of international connectivity have increased. For example, identity verification requirements in New Zealand’s Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) law are part of a global stance, and General Data Protection Regulations (GDPR) emanating from Europe are affecting organisations worldwide in how they manage personal information.

27. The digital environment is rapidly evolving and increasingly dynamic, requiring a more sophisticated understanding and new tools to manage citizens’ digital rights and protect them from threats:

27.1 Identities are evolving into a more complex construct – a web of personal data provided, collected, and shared across multiple people, devices, and entities.

27.2 Citizens’ and organisations’ increased digital activity and sharing of personal data has been accompanied by increased cyber-attacks, fraud, manipulation and privacy threats. Citizens and organisations require better control over their digital identity to participate safely and securely in the digital world;

27.3 Government and business transformation initiatives require digital identity to deliver on their outcomes (e.g. the New Zealand Customs Service relies on effective digital identity for its customs and border operations); and
27.4 Technology is changing quickly as software is more connected than ever; linking people’s social, financial and physical activity together and also biometrically connecting them to their devices.

28. The RealMe suite of services has struggled to keep up with this dynamic environment:

28.1 RealMe is often criticised for its customer experience. Elsewhere, use of social logins or mobile device-based logins are commonplace, and biometric and brokered solutions offer user convenience and control in identity provision. These experiences raise the bar for citizen expectations.

28.2 Resistance to payment for RealMe Login services and slower than expected uptake of the RealMe IVS by agencies and private sector organisations has meant that RealMe has been unable to recover costs, as was originally intended. After $140m of Crown funding, RealMe currently has 500,000 verified identities and supports around 700,000 people logging in and 15,000 asserting their verified identity a month, mostly for Ministry of Social Development StudyLink services.

29. An unregulated market of services has emerged to try and meet the digital identity challenges. Local and international identity providers are offering bespoke digital identity solutions for people in New Zealand. A list of private sector providers is included in the Feasibility Study (page 36) and includes the likes of Centrix and Data Zoo. However, the market is still immature and the services are inconsistent, disconnected, and incomplete.

30. Identity service providers, and organisations in both the public and private sectors that rely on identity services, are looking to government to take the lead in changing this environment. Government is both a large source of authoritative identity data and a significant user of identity services. The private sector want to work with the Government to develop fit-for-purpose services, within a coherent operating model and clear regulatory and policy framework.

31. It is clear that there is an ongoing role for government in digital identity. This view is shared by comparable jurisdictions, such as Australia, the United Kingdom and Canada. Government’s current role is a main digital identity service provider. The Government’s role may change over time to that of a strong regulator, as the market matures and as citizens’ appetite increases for more convenient and integrated services across both the public and private sectors. However, it is likely that citizens will continue to expect highly trusted access to government services and that government will take appropriate steps to ensure that their personal data is security and privacy protected. Given citizens’ high expectations about how government handles their personal data and increasing concerns about cyber security and privacy, this ongoing government role is vital to maintaining citizen trust.

Do nothing scenario

32. Without a change in the Government’s approach, the unregulated market will continue to operate, but:
32.1 Government will continue to invest in the operation and development of RealMe services without acknowledging the emerging market or providing the utility or experiences that citizens and organisations need;

32.2 Government funding of RealMe, and expectations that agencies use it, will continue to crowd out the market, inhibiting natural innovation in solution development and market efficiency;

32.3 There will be potential productivity lost through an increase in the inefficient duplication of processes across government and non-government online services (e.g. to manage siloed identities), and confusion for citizens through inconsistent digital identity processes;

32.4 The expected trajectory is that citizens will continue to be laboured with time-consuming and repetitive processes, challenged in making decisions that affect their privacy, and ultimately be less able to participate effectively in the digital economy.

What we propose to do

33. We recommend that officials continue their work with citizens, agencies, and the private sector to develop options for a new approach to digital identity, including the long term role of government and the private sector in the provision of digital identity services, and to identify regulatory requirements.

34. The work programme would comprise three main work streams – Policy Development, Test and Design Working Examples, and Engagement and Transition.

35. Under the Policy Development work stream, officials would co-design requirements for a Digital Identity Trust Framework with citizens, public agencies and the private sector. The Framework would set the standard for digital identity in New Zealand, ensuring all users have a safe and secure way of connecting with government and non-government services (e.g. banking) online. Any government or non-government agency wanting to provide digital identity services would need to meet requirements set out in the Framework, for example to be an accredited provider. Under this work stream, officials will also complete a comprehensive map of policy that impacts digital identity and privacy and identify regulatory gaps and options.

36. Under the work stream, Design and Test Worked Examples, officials will explore and recommend options on the future role of government in the provision of digital identity infrastructure and services. Officials will lead the co-design and test commercial operating model options and worked examples with users, agencies and private sector interests. The work stream will use user-centric service design in discovery or proof-of-concept projects to investigate improvements to digital identity examples.

37. The Engagement and Transition work stream will bring together public agencies and the private sector, and consult with citizens, to develop options and a proposed way forward. The work stream will also help identify how RealMe products could be repurposed to support the operating model options and the potential implications for agencies. Subject to Cabinet decisions, this work would inform a change management strategy and agency transition plan.
38. The strategic direction for RealMe and associated transition costs will be aligned with the proposed work programme. The actual development of RealMe will be carried out by the DIA RealMe team with its own budget.

**Benefits and risks of developing a new approach to digital identity**

39. The benefits of moving towards a new co-designed operating model for public and private digital identity services are significant. New Zealand will be in a better position to respond to the new challenges in digital identity. People will be able to participate more easily and with greater confidence and choice, businesses will be more empowered to innovate with clarity around the regulatory framework, productivity will improve through reduction of waste, and we will be able to better adapt to challenges that are current (such as AML/CFT compliance) and those that are yet to arrive. The result will be a robust, reliable and resilient digital identity environment that should cost the Government less in the long run.

40. For agencies, there will be the ability for wider utilisation of agency investment already made in digital identity services such as voice biometrics in Inland Revenue and facial recognition in Immigration New Zealand. Agencies will also have a wider choice of digital identity services to meet their customer needs. This will help support an increase in the number and types of digital services that agencies offer. Agencies will also be able to reduce costs as clients will have less need for non-digital contact (e.g. phoning to reset a password).

41. Specific examples of how a robust digital identity approach will enable agencies to solve current pain points include:

41.1 Ministry of Social Development (MSD) currently has to process four to eight sets of manual evidence to be able to grant superannuation for a person turning 65 (income evidence, date of birth evidence, proof of immigration status, and bank statements, as well as other potential evidence such as relationship status, health or housing records). Through digital identity attribute sharing, MSD is considering how this process can be made easier for citizens, and how the integrity of the information involved can be improved.

41.2 Ministry of Health is currently looking at options to safely facilitate information sharing, so that patients and providers can have access to the required health information when and where needed. It has set up a Technical Working Group to explore the use of digital identity as an enabler for broader access and interoperability.

41.3 The Ministry of Education is working with sector and industry partners to enable simpler digitally delivered assessments, enrolment in tertiary institutions, and equitable digital access by leveraging robust digital identity systems and processes.
42. The primary risks of this proposed new direction are that the Government’s long term strategy is unclear (undermining investor confidence), citizen understanding is variable (undermining public trust and confidence in moving to a new approach), or that transition to a new approach is too difficult (leading to cost and delay). Each of these risks can be addressed by the proposed work programme and are outlined more fully in the Feasibility Study. The process will be iterative and, as discussed at paragraph 51, Ministers and Cabinet will make decisions and announcements throughout the delivery of the work programme.

**Contribution of digital identity to the Government’s strategic direction**

43. Digital identity is a whole-of-economy issue and one that needs scale, innovation and investment. As a regulator, the Government has a key leadership role to play to ensure the importance and potential of digital identity is realised. Moreover, digital identity is a core infrastructure component for the Government’s priorities:

- 43.1 to provide for digital rights and digital inclusion;
- 43.2 to close the digital divide by 2020; and
- 43.3 for ICT to be the second largest contributor to GDP by 2025.

44. Because it will improve people’s online experiences, the proposed work programme for digital identity supports the Government’s priorities to share New Zealand’s prosperity and to build a productive, sustainable and inclusive economy.

45. Officials will align the work with the Government Chief Data Steward and other digital and data work underway across government such as in digital rights, life events, digital government and digital inclusion.

**Release of the remainder of tagged contingency budget without the requirement to do a business case**

46. Funding of $1 85 million was drawn down in July 2017 to investigate a business case for the transition to a digital identity marketplace. The business case was to be the trigger for the release of the remainder of the contingency.

47. As the work progressed, it became increasingly clear that a full business case, presenting a detailed and costed permanent solution to digital identity would not be appropriate or possible, and an iterative and explorative approach is preferred instead.

48. The attached *Feasibility Study* uses the business case template to the extent possible. It focuses on the strategic and economic cases. The strategic decisions sought in this paper do not lend themselves to the preparation of commercial, financial and management cases.

49. The broad conclusion of the work to date is that the Government should explore the government-dominated supply of digital identity services and expectations about the use of those services. A digital identity market is emerging and the RealMe set of services are a barrier to its development.
50. Officials are seeking Cabinet approval to release the remainder of the contingency funding to continue the work. An agile and iterative approach is required with appropriate checks and balances.

51. The work ahead will include policy, design and deliverable decisions that will need to be made progressively as new information is generated through iterative processes and engagement. These decision points will include whether to continue, change direction, or conduct further work to inform the next phase. The work will determine the extent to which, and how, the Government needs to be involved at any point of time.

52. We recommend that Cabinet rescind the requirement to prepare a business case and approve the release of the remaining $5.15 million of contingency funding to continue the work.

**Delivering the proposed work programme**

53. We recommend that officials be directed to develop a detailed work programme to deliver a new approach to digital identity, establish appropriate governance – including an independent advisory group comprising senior officials and private sector members – and outline wide public engagement. The work programme will detail and update the description of work in this paper and also Appendix VI of the *Feasibility Study*. Recognising the sensitivity and risks associated with proposed work programme, officials will be guided by the following principles that are aimed at enhancing citizens’ trust and confidence in how the Government handles their personal data:

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer centric</td>
<td>Better customer experience is a driver behind all options</td>
</tr>
<tr>
<td>Privacy and security by design</td>
<td>Privacy, security and citizen control and consent ‘baked in’ from the beginning of the process</td>
</tr>
<tr>
<td>Open and transparent</td>
<td>Wide consultation and co-design with citizens and other stakeholders; transparency of decision making</td>
</tr>
<tr>
<td>Meets broad stakeholder needs</td>
<td>Balances the needs of a wide range of stakeholders</td>
</tr>
<tr>
<td>Interoperability</td>
<td>Ensures interoperability with comparable jurisdictions</td>
</tr>
</tbody>
</table>

54. Officials will report to the Minister of Finance, Minister for Government Digital Services, Minister of Internal Affairs and Minister of Commerce and Consumer Affairs. Ministers will oversee the work programme, and take decisions for referral to Cabinet.

55. The work will be led by the transition team, independent of RealMe. The RealMe work will be carried out by the DIA RealMe team. The transition team will be closely involved to support and align the RealMe work with wider digital identity work.

56. Officials have completed high level costings and believe the work programme can be delivered with the remainder of the contingency funding of $5.15m over two financial years. The funding will cover 8-10 core staff, and additional resourcing of specialists over the life of the programme, collaborative development of use cases to test assumptions and prototype solutions, overheads and public engagement.
<table>
<thead>
<tr>
<th>Programme outputs</th>
<th>Phase 1</th>
<th>Phase 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sep-Dec 2018</td>
<td>Jan-Jun 2019</td>
</tr>
<tr>
<td>Governance/accountability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirm work programme and timeframe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report to Ministers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish Independent Advisory Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Final Cabinet report</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Policy Development</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cabinet approval of consultation document on initial proposals for Digital Identity Trust Framework (DITF)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public consultation on DITF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report back to Cabinet with proposed final DITF and next steps/implications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Release high level DITF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy implications of new approach (options)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cabinet update and decisions on policy implications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legislative reform (if required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Design and Test Worked Examples</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proof-of-concept/discovery projects</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop system requirements and technical standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ministerial consideration of technical system options</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Engagement and Transition</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic models for Crown &amp; commercial participants</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public and stakeholder engagement plan for approval, and implementation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transition implications and plan for agencies</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RealMe – Separate from but aligned to the Work Programme</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RealMe strategic alignment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation of RealMe decisions</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Consultation</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
57. The following agencies were consulted and are in general agreement with the new approach to digital identity recommended in this paper: Accident Compensation Corporation, Department of Corrections, Department of Internal Affairs, Department of the Prime Minister and Cabinet (National Cyber Policy Office), Government Communications Security Bureau, Inland Revenue, Land Information New Zealand, Ministry of Business, Innovation and Employment, Ministry of Education, Ministry of Health, Ministry of Justice, Ministry for Primary Industries, Ministry of Social Development, New Zealand Customs Service, New Zealand Transport Agency, Office of the Privacy Commissioner, State Services Commission, Statistics New Zealand, The Treasury. The Department of the Prime Minister and Cabinet (Policy Advisory Group) has been informed.

**Financial implications**

58. This paper seeks the release of the remainder of the contingency funding ($5.15 million) to continue work on developing a new approach to digital identity.

59. §(2)(f)(iv)

60. Longer-term funding implications, including transition costs, will be included in the report back to Cabinet by October 2020.

**Human rights**

61. All proposals in this paper are consistent with the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993.

**Legislative implications**

62. There are no legislative implications arising from this paper. Legislative implications will be identified through work on the Digital Identity Trust Framework and reported to the Ministers’ Group and Cabinet by October 2020. For instance, changes to the Electronic Identity Verification Act 2012 may be required to allow greater involvement of the private sector in the provision of digital identity services.

**Publicity**

63. Subject to Cabinet approval we intend to publicly announce the digital identity work programme and our intention to seek stakeholder involvement in its delivery.

**Recommendations**

64. The Minister for Government Digital Services and Minister of Internal Affairs recommend that the Cabinet Economic Development Committee:

1. note that:
1.1 Budget 2017 established a tagged contingency of $7 million for the development of an alternative digital identity solution for New Zealand;

1.2 funding of $1.85 million was drawn down in July 2017 to develop a business case for the transition to a digital identity marketplace; and

1.3 the Minister of Internal Affairs was invited to report back to Cabinet in December 2017 with a business case outlining the proposed transition and seeking drawdown of the remainder ($5.15 million) of the contingency [CAB-17-MIN-0185.13];

2. **note** that officials have undertaken analysis across the New Zealand public and private sector landscape, and internationally, and prepared the attached Feasibility Study (using as much of the business case template as possible given the iterative nature of the work);

3. **agree** that in recognition of the emerging market in digital identity services, the Government will continue working with citizens, agencies and the private sector to develop options for a new approach to digital identity, including the long term role of government and the private sector in the provision of digital identity services, and identify regulatory gaps;

4. **note** that because there are sensitivities with how the Government handles individuals’ personal data, the work programme will be guided by principles that place a heavy emphasis on citizen consent and control: Customer centric; privacy and security by design; open and transparent; meets broad stakeholder needs; and interoperability;

5. **direct** officials to prepare a detailed work programme that will include: development of a Digital Identity Trust Framework to set the standard for digital identity in New Zealand, and other policy work; design and test worked examples; engagement and transition (including implications for agencies); governance and oversight arrangements;

6. **agree** that the work programme will be approved and its delivery overseen by the Minister of Finance, Minister for Government Digital Services, Minister of Internal Affairs and Minister of Commerce and Consumer Affairs;

7. **invite** the Minister for Government Digital Services and the Minister of Internal Affairs to report back to Cabinet by October 2020 on the outcomes of the work programme and any longer-term funding implications, and to report earlier as necessary to seek Cabinet decisions at key points to enable the work to progress;

8. 8(2)(b)(iv)

9. **recede** the previous Government’s Cabinet decision [CAB-17-MIN-0185.13] requiring a business case to release the remainder of the tagged contingency funding ($5.15 million); and instead;
10. **approve** the following appropriations to meet the Department of Internal Affairs costs of continuing work to establish a digital identity ecosystem, with a corresponding impact on the operating balance:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Category Expenses and Capital Expenditure: Civic Information Services MCA Departmental Output Expense: Managing and Accessing Identity Information (funded by revenue Crown)</td>
<td>2.575</td>
<td>2.575</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

11. **agree** that the proposed changes to appropriations for 2018/19 in recommendation 10 above be included in the 2018/19 Supplementary Estimates and that, in the interim, the increases be met from Imprest Supply;

12. **agree** that the expenses incurred under recommendation 10 above be a charge against the “Transition to a Digital Identity Marketplace” tagged contingency, established as part of Budget 2017;

13. **note** that subject to Cabinet approval to the recommendations above, we intend to announce the digital identity work programme and seek the involvement of citizens and other stakeholders in its delivery.

Authorised for lodgement

Hon Dr Megan Woods
Minister for Government Digital Services

Hon Tracey Martin
Minister of Internal Affairs
Appendix A: Feasibility Study for a New Approach to Digital Identity

Prepared by: Digital Identity Transition Team
Date: 26 September 2018
Version: 1
Status: Final
## Contents

**Executive summary** ........................................................................................................... 3

**Introduction** ...................................................................................................................... 9
  - Structure and purpose of this document ................................................................. 9
  - What is digital identity? ............................................................................................ 10

**Strategic case** .................................................................................................................. 11
  - Strategic context ........................................................................................................ 11
    - Government’s interests in digital identity ........................................................... 11
    - Government’s current role in the provision of digital identity services .............. 11
    - Shifts in the operating environment .................................................................... 14
    - What are the choices for the future role of government in digital identity? ....... 16
  - Organisational overview ........................................................................................... 17
    - Alignment with Government’s strategic direction ............................................... 17
    - Alignment with international approaches ............................................................ 18
  - Benefits, risks, constraints and dependencies ....................................................... 19
    - Main benefits ........................................................................................................ 19
    - Main risks ............................................................................................................. 21
    - Key constraints and dependencies ..................................................................... 23

**Economic case for change** .............................................................................................. 25
  - Problem definition ..................................................................................................... 25
  - Critical success factors ............................................................................................ 25
  - Long-List options and initial assessment .................................................................. 26
    - Government Exits ................................................................................................. 26
    - Government as a service provider ....................................................................... 27
    - Collaborative model – joint service provision ..................................................... 28
    - Government as regulator and standard setter only .............................................. 28
  - Assessment of Long-List options ............................................................................. 28

**Recommended strategic direction** ................................................................................... 30
  - Next steps .................................................................................................................. 32

**Appendix I: Key stakeholders engaged** ........................................................................... 33

**Appendix II: Sample global research** .............................................................................. 35

**Appendix III: Provider Market Scan** .............................................................................. 36

**Appendix IV: Delivery Dimensions for Long-List Options** ............................................ 37

**Appendix V: Assessment of Long-List Options** .............................................................. 38

**Appendix VI: Digital Identity Programme Value Map** .................................................... 44
Executive summary

1. The ability to prove one’s identity is the basis for participation in social, political, economic, and cultural life. Digital identity underpins trust in the digital world.

2. New Zealand has an opportunity to establish a new approach to digital identity that effectively protects the security and privacy of citizens’ personal data, maximises the value of government investment, ensures that secure and fit-for-purpose solutions are available, and has the flexibility to address the diversity of current and future needs.

3. This Feasibility Study establishes the case for change, lays out the strategic context, and assesses a long list of options developed in consultation with agencies. It concludes that a new and collaborative approach to digital identity is required to better understand the core elements of an adaptive and flexible future digital identity ecosystem.

4. The work to prepare this study has included a wide scan of international experience (including detailed consultation with government initiatives in Australia, the United Kingdom, and Canada), Investment Logic Mapping with agencies, and extensive engagement with private sector enterprises.

5. The Study stops short of a business case because, at this stage of its evolution, the preferred option can only be a strategic direction within which there remain numerous variables and dynamic externalities. While there is clarity in the overall objectives and the principles underpinning the approach, the processes and engagement required to produce the information needed for key decisions are iterative and occur within a rapidly changing environment.

6. Key design and deliverable decisions will need to be made progressively as new information is generated (e.g. decisions about the extent to which and how the Government needs to be involved at any point of time). Dealing with uncertainty requires a flexible and phased approach. Decision points will include whether to continue, change direction, or do further research/work/consultation to inform the next phase of work.

7. A high level work programme is outlined that includes the development of a Digital Identity Trust Framework and other policy work, ecosystem design (e.g. co-design a market operating model), transition (including impacts on and implications for agencies), engagement, governance and oversight arrangements.

---

1 For the purposes of this Feasibility Study, citizen refers to an individual using digital identity services in New Zealand regardless of their citizenship status.
**Digital identity is a critical enabler of a digital nation**

8. Digital identity is an electronic representation of an individual. It provides a means for people to undertake online what they have traditionally done manually – for example applying for benefits, opening bank accounts, retail shopping and renewing a passport.

9. An effective digital identity system, while not an end in itself, has the potential to unlock significant new opportunities for citizens, the economy and for society as a whole. Digital identity is a key foundational piece of government efforts to: ensure digital rights; increase digital inclusion; grow the digital economy; and accelerate digital transformation across the public sector.

**The current approach to the delivery of digital identity services is no longer sustainable**

10. Since 2011, the Government has taken a lead role in the direct provision of digital identity services for New Zealanders. RealMe services are recognised internationally for their strength and reliability. The services include:

   10.1 RealMe Login – supports citizens to use the same login to access multiple government services using a single username and password; and

   10.2 RealMe Identity Verification Service (IVS) – provides a mechanism for ensuring that people are who they say they are online. The IVS provides a universal high level of assurance to agencies and businesses.

11. The integration of services with broad customer bases (e.g. StudyLink), recent improvements to the application process for identity credentials, and growing citizen awareness of the importance of digital identity “strength”, have resulted in steadily-increasing numbers of people obtaining and using RealMe IVS for government services. The development of ‘RealMe Now’, a way of on-boarding instantly through a mobile phone, will assist to improve service accessibility.

12. However, despite recent growth and innovations, private sector uptake and the number of services using IVS remain low. Government transactions alone lack the scale to make the current model affordable or sustainable in the long term. The breadth and diversity of public and private sector digital identity demands, including the need for choice and citizen-centric design, are outpacing the ability of RealMe to deliver.

13. Digital identity is increasingly seen as a whole-of-economy issue, and one that needs scale, innovation and investment from the private sector. At the same time, citizen expectations are increasing based on their interactions with private sector digital services, concerns about the privacy and security of information, and changes in technology (e.g. biometrics, blockchain and mobile services).

---

2 Levels of assurance are classified on a scale of 1 to 4, with level 4 being the highest. Very few transactions require level 4 assurance, one example being the issuance of a passport. RealMe IVS provides a level 4 assurance.
14. Some government agencies are working around RealMe, seeking alternative solutions that better meet their digital identity needs and are more responsive to citizen preferences. This practice reduces the effectiveness and coordination of overall government investment.

15. Independent reviews\(^3\) of RealMe have been undertaken in response to concerns about lower than forecast adoption rates, customer service issues and fragmented and inefficient investment. The reviews pointed to the need for a shift in approach, recognising that RealMe is unlikely to ever be self-funded through user fees (and would therefore require significant ongoing government funding) and that the private sector market in digital identity services is rapidly evolving. Subsequent research\(^4\) concluded that a nascent market in digital identity solutions exists, and that it could meet some of the identity verification needs of government and citizens, particularly at lower levels of assurance.

16. Budget 2017 established a tagged contingency of $7 million for the development of an alternative digital identity solution for New Zealand \[\text{CAB-17-MIN-0185.13 refers}\]. Funding of $1.85 million was drawn down in July 2017, following the establishment of an independent transition team\(^5\) to investigate and develop an indicative business case for a new approach to digital identity.

**A collaborative digital identity ecosystem offers significant potential**

17. This Feasibility Study canvases a range of approaches for the future of digital identity service provision in New Zealand. Options have been grouped into three categories:

17.1 **Exit** – a complete exit of all current functions associated with digital identity;

17.2 **Government as a service provider** – a continuum of options where the government remains the primary provider of digital identity services, centred on the continuation/development of RealMe; and

17.3 **A collaborative ecosystem between the public and private sectors** – which recognises the reality that digital identity is a whole-of-economy issue, and where government maintains provision of a high-level identity service (RealMe IVS) while working with the private sector to create the conditions to ensure other identity products and services are available. This option could lead to government’s primary role in digital identity becoming a standard setter and regulator, if the market matures sufficiently and the risk profile is appropriate.

\(^3\) Reviews by: Gravelroad (2014); X4 Consulting (2015); and Inflection (2015)

\(^4\) Deloitte (2016)

\(^5\) The transition team comprises a mix of resources from across government agencies, together with expert knowledge holders.
18. An immediate and complete government exit from the provision of digital identity services is not a viable option, as the market is not yet mature enough to provide all of government’s digital identity needs and the risks to citizens, to public and private sector organisations, and to government itself, are not tenable.

19. Options to maintain or develop the Government’s role as a primary provider of digital identity services (via RealMe) have been considered. However, these are unlikely to meet the expectations of citizens, or the needs of public and private sector digital identity service providers.

20. Analysis across the New Zealand public and private sector landscape, and internationally, supports a transition to a “Collaborative Digital Identity Ecosystem”. Figure 1 depicts the model of collaboration to be taken to deliver the work. In this scenario, government would gradually divest itself as a provider of login services while evolving IVS services to complement digital identity services provided by others at lower levels of assurance. This transition would need to allow time for alternative private sector digital identity services to develop coherently, and for citizens, agencies and businesses to switch to new providers.

![Figure 1: Model of collaboration](image)

21. To establish coherence and trust, the ecosystem would be governed by a set of system rules (a Digital Identity Trust Framework) allowing citizens and organisations to interact securely, and with confidence, because authoritative sources establish and verify their identities. It would also provide the public and private sectors with a

---

shared, sustainable and cost-effective operating platform, supporting digital identification and authentication.

22. Ultimately, the market may mature to a point where new digital identity service providers are able to meet the full range of user needs, including high level identity verification services currently only offered by RealMe IVS. At this point, if risk appetite allows, the Government would have the option of completely exiting digital identity service provision, and focusing on its regulatory and standard setting roles only.

23. Comparable international jurisdictions (Australia, Canada and the United Kingdom) are also looking for universal digital identity solutions, motivated by a similar set of drivers. In each case, work is at an early stage of development and there is a willingness to cooperate with New Zealand to resolve common issues and, where appropriate, promote interoperability across jurisdictions.

24. In addition, digital identity is a key enabler for initiatives aimed at developing a single Trans-Tasman economy, such as the National Business Number (NBN) and “e-invoicing”. Alignment of digital identity standards across the Tasman will be necessary to support this work.

**Strong public and private sector support for a collaborative approach**

25. The transition team has engaged extensively with public and private sector stakeholders to better understand their digital identity needs and to test the appetite for a collaborative approach to developing solutions. The concept has been met with strong support from all parties.

26. It has become clear that digital identity is a whole-of-economy issue. The private sector demand to consume digital identity services is significant and growing – driven in large part by the need to comply with legislation such as the Anti-Money Laundering and Countering Financing of Terrorism Act 2009.

27. Banks and other private sector organisations have pursued their own digital identity solutions, seeking to improve New Zealanders’ online experiences, while also reducing fraud, protecting against cyber-attacks, mitigating regulatory risks and lowering transaction costs associated with accurately establishing an individual’s identity. However, they are yet to identify a complete answer that addresses all of their concerns to the standard that they require.

28. The banking sector does not want to compete on digital identity solutions; rather it wants to collaborate with the Government and is willing to invest in the development of effective digital identity solutions for all of New Zealand. Strategic partnerships with the private sector – leveraging expertise, co-ordinating investment, and consolidating volumes and frequency of digital identity transactions across the economy – will maximise benefits for New Zealand as a whole.
29. The momentum for change is growing. The transition team is holding in-confidence discussions with and all the major banks about joint projects that would test and demonstrate how major parties can participate in multiple ways within a collaborative digital identity ecosystem to solve real business compliance problems. Others, such as Auckland City Council, are also keen to work alongside the transition team to address burgeoning operational needs. The ability to collaborate and work in an agile way across the public and private sectors is a significant advantage evident in New Zealand and not mirrored in other jurisdictions.

30. Public sector agencies have reported a need for a wider range of identity attributes, beyond the standard identifiers commonly used, and are also very encouraging of a shift to a united approach. Agencies have expressed their support for working collaboratively on use-cases that rapidly investigate, test and prove how digital identity could enable easier, more efficient interactions for citizens and enhance access to services.

**Tagged contingency funding is required to support the next phase of work**

31. Cabinet agreement is required for the release of the remaining $5.15 million of the tagged contingency fund to support the transition team to complete the next phase of work, focused on designing and testing key elements of the new approach in collaboration with citizens and other key stakeholders. Actions will include: defining the requirements of a supporting technological platform; working alongside a broad group of stakeholders to develop a Digital Identity Trust Framework; and ongoing proof of concept testing and prototyping. This stage of the project will be underpinned by consultation and citizen engagement, and partnering with the public and private sectors to leverage collective expertise and resources, to develop the detail of system components.

32. Officials will report to a ministerial governance group. The ministerial group would oversee the progress of the work and bring papers to Cabinet at key decision points. It is also recommended that the transition team be directed to report to Cabinet by June 2020 on the outcomes of its work.
Introduction

Structure and purpose of this document

33. Budget 2017 established a tagged contingency of $7 million for the transition to a Digital Identity Marketplace [CAB-17-MIN-0185.13 refers]. Funding of $1.85 million was drawn down in July 2017, following the establishment of an independent transition team to prepare the business case for a new approach.

34. This Feasibility Study tests the case for a new approach to support the ongoing development and testing of a collaborative ecosystem for digital identity. This approach offers a feasible and forward-facing solution to digital identity that will deliver value to New Zealanders, and to the economy as a whole.

35. The emphasis in this Feasibility Study is on the strategic and economic cases, with a lesser focus on the financial, commercial and management aspects at this stage.

36. The purpose of this Feasibility Study is to:
   36.1 articulate the case for change;
   36.2 confirm the feasibility of the collaborative digital identity ecosystem concept as an approach that provides citizens with a convenient, secure and trustworthy means of proving their identity online;
   36.3 confirm the strategic context and fit of the proposed approach;
   36.4 recommend that work continue with citizens, private sector and government agencies to design, build and test aspects of the collaborative digital identity ecosystem model; and
   36.5 seek Cabinet approval for the release of the remaining $5.15 million for the ongoing development of the collaborative digital identity ecosystem, with the transition team to report to Cabinet by June 2020 (if not earlier) on the outcomes of its work.

37. The transition team has worked closely with key stakeholders spanning the public and private sectors to develop the Feasibility Study. Facilitated workshops and investment logic mapping processes have been used to gain an in-depth understanding of agency and business needs and interest, and to clarify the potential utility of a digital identity solution that will serve multiple interests.

38. Approaches taken in comparable international jurisdictions have also been researched and the transition team has consulted directly with key players in Australia, Canada and the United Kingdom. A full list of those engaged is attached at Appendix I.
What is digital identity?

39. Identity is vital to everyday life. Valid identification is a prerequisite for accessing and participating in society, such as banking, voting, travelling, and healthcare. An individual’s identity is a representation of them as unique and distinct. Depending on the context, the representation can use personal attributes, such as name, date and place of birth, each linked to the individual.

40. Fundamentally, digital identity is critical to the digital future because it underpins trust and accountability for transactions. It is the key to a safe and secure digital world, allowing people to undertake online what they have traditionally completed manually so they can participate in our modern digital economy and society.

41. New Zealanders are already undertaking multiple digital transactions on a daily basis – interacting with friends, family and communities on social media, banking online, purchasing products, and paying taxes. As a result, many of us have multiple digital identities. These identities can extend to a variety of data attributes, such as photos, address, credit rating and income, all of which have been associated with or shared by the individual at some time.

42. Key activities in the digital identity process are:

   Figure 2: The digital identity process

<table>
<thead>
<tr>
<th>Identification</th>
<th>Authentication</th>
<th>Assurance</th>
<th>Authorisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish identity</td>
<td>Confirm identity</td>
<td>Assert identity</td>
<td>Use identity</td>
</tr>
</tbody>
</table>

| Identification | The process of establishing or verifying information about an individual, through proving ownership of official documents (e.g. driver’s licence, passport), consulting alternative data sources to corroborate the identity being claimed, and/or collecting biometric data from the individual to link them to source records. |
| Authentication | The process of confirming a previously established identity, usually to log on and reuse a service, by presenting a credential such as username and password. This demonstrates the person is in control of the digital identity recognised by the service provider. |
| Assurance | The process of giving confidence in the authenticity of an identity such as by asserting details previously established during identification. The strength of verification in the identification process will determine the level of assurance given. |
| Authorisation | The process of determining what actions may be performed or services accessed on the basis of the identity. |

43. A selection of global research papers into digital identity is listed in Appendix II.

---

7 Consult Hyperion (2016) *Digital Identity: Issue Analysis*
Strategic case

Strategic context

Government’s interests in digital identity

44. Digital identity, while not an end in itself, is a critical enabler of effective and efficient service delivery across the public, private and non-government (NGO) sectors, and a facilitator of citizens’ engagement in digital society more generally. The verification of identity is therefore central to the activities of government, business and citizens.

Government’s current role in the provision of digital identity services

45. Factors influencing the approach to digital identity adopted by governments around the world include whether or not the country has a mandatory population register (as in Denmark, Norway and Estonia), and the extent to which key identity data is centralised (as in Denmark) or spread across multiple agencies at multiple levels of government (as in the United States).

46. Some jurisdictions have introduced compulsory national identity cards with success. For example, the Estonian ID card can be used as a driver’s licence, a virtual ticket on public transport, a travel document around the European Union, a health insurance card, and to access government databases such as health records and taxes.

47. However, in general terms, these countries have significantly different cultural and political profiles to that of New Zealand and other Westminster-style governments. Past attempts to introduce the compulsory ID card concept in the United Kingdom and Australia have been met with strong public resistance on the basis of individuals’ privacy and security concerns. New Zealand’s privacy settings prohibit the re-use of unique identifiers for individuals. There is also strong evidence, from the Office of the Privacy Commissioner and others, that there is no social licence for a population register type approach in New Zealand.

RealMe is government’s mandated digital identity service

48. For over a decade, the New Zealand Government has played a significant role as a direct provider of digital identity products (through the RealMe suite), with a limited standard setting function. This approach was driven by the fact there were gaps in the market provision of digital identity products and services at the time decisions were made. It was also driven by a belief that digital identity is a core infrastructure component for the digital nation New Zealand wants to become.

49. The Government became a direct provider of digital identity services in an effort to improve New Zealanders’ experiences of digital government. In 2006/07 the Government developed the ‘Government Logon Service’ (later branded ‘RealMe Login’), in response to concerns about the proliferation of government websites, each requiring a unique login procedure. RealMe Login allows citizens to access multiple government services using the same username and password.
50. In 2008/09 the Government introduced the iGovt identity verification service, providing a mechanism for ensuring that people are who they say they are online. The service was rebranded and launched as the RealMe Identity Verification Service (IVS) in July 2013. The IVS provides a universal ‘high’ level of assurance to agencies and businesses that require it. The RealMe products have been designed to protect the privacy of users and to allow users to retain control over who accesses their identity information.

51. Government mandated the use of these identity services across the public sector, in an effort to ensure consistency in approach by agencies, and to maximise economies of scale and prevent unnecessary duplication of the Crown’s investment. The overarching vision was for a unified all-of-government approach to digital identity, offering citizens a seamless experience when interacting with government online.

52. At the time that the login service and IVS were developed there were no alternative commercial providers in New Zealand. It was anticipated that the private sector would also take-up the IVS and, in doing so, contribute to the costs of identity service provision. This has not proved to be the case.

53. In 2011, the Department of Internal Affairs entered into a partnership with New Zealand Post (NZ Post) in a bid to drive private sector demand for the IVS. The partnership also allowed for the use of the NZ Post distributed network of retail outlets for people to bring their primary identity documents (e.g. passports and birth certificates) to be verified and to have a photograph taken to link them to their photograph on record. The partnership was recently ended by mutual agreement, as the uptake of RealMe services by the private sector had not met expectations.

54. Government continues to play multiple roles as product developer, provider and investor in the multi-sided digital identity marketplace.

**Demand for RealMe services has not met expectations**

55. Despite efforts to stimulate both public and private sector demand for RealMe identity services, the result has fallen well short of projections. Citizens, public sector agencies and private sector organisations have all been slow to take up RealMe identity services for a range of reasons:

55.1 the ‘one-size-fits-all’ IVS product offering a high level of assurance (level 4) exceeds the requirements of the majority of government agencies, who have assessed their assurance needs to be lower;

55.2 the IVS product is viewed by agencies and private organisations as difficult to integrate with their own operating systems; and

---

8 Levels of assurance are classified on a scale of 1 to 4, with level 4 being the highest. Very few transactions require level 4 assurance, one example being the issuance of a passport, although level 4 is provided by RealMe IVS.
55.3 RealMe products lack the flexibility and mobility that citizens expect in the current online environment:

- the login service has limited utility to many citizens – on occasions when they are required to use it, the experience can be frustrated by an inability to recall a password, and may result in the need for contact centre assistance; and

- RealMe IVS does not yet provide an end-to-end digital experience for users, requiring citizens to take manual steps to establish their identity (although ‘RealMe Now,’ a way of on-boarding instantly through mobile phones, is live for new Kiwibank customers).

56. The mismatch between public sector agency needs and the services offered by RealMe has led to some agencies working around RealMe, and using alternative digital identity services that better meet the needs of their customers. This effectively undermines the Government’s vision of a coherent and integrated user experience, and has resulted in the fragmentation and duplication of investment.

57. While the appetite to do so is strong, a history of siloed approaches and legacy platforms makes it hard for agencies to adopt RealMe efficiently. Timing, governance and funding constraints further prevent agencies from ‘always doing the right thing’.

---

**Figure 3: Snapshot of RealMe uptake**

- **Current RealMe IVS Uptake – a snapshot**
  - seven public sector agencies use RealMe IVS, applied to nine services
  - the two major public sector users are the Department of Internal Affairs (passport applications) and the Ministry of Social Development – StudyLink (Student Allowance and Student Loans)
  - six private sector organisations use RealMe IVS, applied to six services
  - the majority of private sector users access IVS services on a small-scale, comprising a very small portion of the total number of asserted identities (only 7,000 asserted identities since 2012, equating less than 1% of the total assertions)
  - approximately 450,000 New Zealanders have a verified identity. Recent growth in numbers has been driven in a large part by the ability to co-apply for a verified identity at the same time as applying for a New Zealand passport renewal and through StudyLink when applying for a student loan
  - the total number of occasions in which New Zealanders have used IVS to assert their identity is approximately 338,000 – some of which will be duplicates. This reflects the lack of utility of a verified identity i.e. low number of agencies and others using IVS to access their services, providing limited value to citizens.
58. There have been three independent reviews of the current digital identity approach. In 2014, the Department of Internal Affairs (DIA) in consultation with Treasury, commissioned Gravelroad to carry out a review of RealMe costs and benefits. In 2015, Treasury commissioned X4 Consulting to carry out a commercially focused review on whether RealMe was likely to become self-funding through fees and charges. Later in 2015, DIA commissioned Inflection, a Silicon Valley-based company specialising in digital identity, to provide its view of the most appropriate way forward.

59. Collectively, these reviews reflect on changes in the operating environment and point to a need for a shift in approach. While RealMe is a system asset for the public sector, the business model is not sustainable.

60. More recently, DIA commissioned research into the viability of the digital identity market in New Zealand. A 2016 report from Deloitte found that a nascent market in digital identity exists, and recommended that government work with the market to help it fully emerge and mature (a current scan of existing and emerging market providers is listed in Appendix III). It also found that there is a need to continue with a government provided service as the market cannot yet meet all of government’s, or citizens’ digital identity needs.

**Significant investment has been made in RealMe**

61. Contrary to expectations, government has so far had to bear all of the risks and costs of the development and operation of RealMe services. Total Crown funding to date is approximately $140 million.

62. Attempts to charge government agencies for identity service provision have been met with strong resistance. As a result, agencies are only charged for helpline (contact centre) services.

63. This situation has arisen because of the low number of agencies using RealMe IVS and the fact that agencies cannot easily identify the cost of their manual identity processes or extract savings from moving to a digital identity process.

**Shifts in the operating environment**

64. Significant changes in the operating environment have implications for the future provision of digital identity services.

**Alternative private sector suppliers of identity services have emerged**

65. The digital identity environment has shifted dramatically in the past decade. Digital identity solutions are increasingly available on a commercial basis. Logins are commonly used across the private and non government sectors, and new technologies support the linking of services through shared platforms and/or the use of federated models of login, supporting users to access multiple services with a single login.
66. Identity verification is also becoming progressively accessible and user-friendly, as new technologies such as biometrics and mobile offer convenient and secure solutions – potentially at a lower cost. It is difficult for government to keep pace with these changes, yet citizens’ expectations are set by private sector developments.

67. The New Zealand market for digital identity services is small, and the lack of coherence in current investment is costly and inefficient. Government lacks the pervasiveness and volume to make digital identity solutions valuable and cost effective. There is a need to consider digital identity as a whole of New Zealand economy issue.

Citizen expectations of control over personal data are growing

68. Citizens are concerned about the need to protect personal information from privacy and security breaches, and identity theft. A 2016 opinion survey commissioned by the Privacy Commissioner suggested that a large portion of New Zealanders are concerned about issues related to identity theft, credit card and banking details, businesses and government sharing personal information and security of information.

69. At the same time, there is a growing national and international citizen interest in ownership and control of personal data, with citizens demanding greater transparency about what information is held about them and how it is used. The Government has signalled its intention to enhance digital rights and provide a strengthened framework to protect New Zealanders in the online world.

Public sector service delivery is increasingly reliant on identity information

70. Public sector agencies report a growing need for consent-based digital access to a wider range of information about people (e.g. income and address), some which cannot be obtained in a digital format. This places a burden on citizens to provide physical documentation at their own cost, and means that agencies revert to expensive manual procedures to process applications. Such inefficient approaches to digital identity may act as a barrier to service accessibility and contribute to system-wide inequities.

Private sector operators are also looking for digital identity solutions

71. Organisations in the private sector, such as banks, are seeking digital identity solutions that allow them to improve New Zealanders’ online experiences, while also reducing fraud, protecting against cyber-attacks, mitigating regulatory risks and lowering transaction costs associated with accurately establishing an individual’s identity.

---

9 Office of the Privacy Commissioner (2016) Privacy Concerns and Sharing Data (undertaken by UMR Research).
10 For example, when a person applies for financial assistance from the Ministry of Social Development they need to provide at least two certified identity documents, plus five or more documents with supporting individual identity information (depending on the person’s circumstances). These documents need to be provided as physical paper documents and in many cases the applicant will need to contact other government agencies or organisations to obtain the required documentation.
72. The ability to verify identity to a suitable level of assurance is vital if businesses\textsuperscript{11} are to meet their obligations under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009. The cost of compliance with these regulations is likely to be significant, and potentially unsustainable, for smaller players many of whom have not had to grapple with these issues before. A collaborative approach to digital identity would help to ease the compliance burden for small to medium enterprises.

73. The growth of the digital economy is dependent on citizens and organisations being able to transact confidently and with ease in a secure environment, including across international borders. It is therefore important that digital identity solutions adopted in the New Zealand context are compatible with those of our major trading partners.

74. Banks and other large digital businesses have invested in finding their own identity solutions, but are yet to identify a complete answer that addresses all of their concerns to the standard that they require. These businesses do not want to compete on digital identity solutions, and are willing to partner with the public sector to develop solutions for the benefit of New Zealand as a whole. This creates an opportunity for government to help shape the future of digital identity solutions and to encourage collaborative approaches to innovation and investment.

**What are the choices for the future role of government in digital identity?**

75. Government has an enduring interest in ensuring that secure and reliable digital identity services are accessible, and delivered in a way that serves the interests of citizens, the public and private sectors, and New Zealand as a whole. At a minimum, the role of government is to establish the regulatory framework within which digital identity services are offered, and protect the privacy and security interests of citizens and New Zealand as a whole.

76. However, the Government has choices about the role(s) that it plays in the provision and funding of digital identity services within the multi-sided marketplace. At a high-level, the alternatives are:

76.1 **Exit** – a complete exit of all functions associated with digital identity. An immediate and complete exit from RealMe is not a realistic option. It would leave public sector agencies without alternative identity services (particularly high level verification services), disrupting service delivery and inconveniencing citizens.

76.2 In the medium to long term, a lack of government oversight of digital identity services is likely to result in fragmented investment in the design and delivery of identity services, creating inefficiencies and potentially compromising service quality.

\textsuperscript{11} For example banks, lawyers, conveyancers, accountants and real estate agents.
76.3 **Government as a service provider** – a continuum of options where the Government remains the primary provider of digital identity services, centred on the continuation and/or development of RealMe.

76.4 Options in this category may not meet the expectations of citizens, or the needs of public and private sector digital service providers. It is not in the interests of government to continue to invest in services that are fast becoming obsolete.

76.5 **A collaborative ecosystem with the public and private sectors** – where government maintains provision of a high-level identity verification service (RealMe IVS) while working with the private sector to create the conditions where other identity products and services are available.

76.6 A collaborative approach recognises the reality that digital identity is a whole of economy issue. This option could lead to the Government’s primary role in digital identity becoming a standard setter and regulator, if the market matures sufficiently and the risk profile is appropriate.

76.7 This Feasibility Study identifies the collaborative digital identity ecosystem model as the preferred option, offering a flexible and sustainable path forward. (The regulatory and standard-setting only model is not recommended on the basis that it is not achievable or desirable within the current context).

77. A full-list of specific options within this framework is included in the Economic section of this study.

**Organisational overview**

78. Work on the development of options for the continued provision of digital identity solutions to the public sector, and potentially beyond, has been led by an independent transition team (hosted by the DIA). The transition team represents a blend of multiple agency and contracted resources with subject matter expertise.

79. The team draws widely from interested stakeholder groups.

**Alignment with Government’s strategic direction**

80. The proposal to invest in a fit-for-purpose digital identity solution is consistent with the Government’s intent to seize opportunities presented by new digital technologies to drive the transformation of New Zealand society, the economy and government.

81. Digital identity forms part of a broader infrastructure required to support transformative change. The proposed way forward aligns with specific government priorities, as follows:

81.1 *improving digital inclusion and closing the digital divide by 2020*;
An easy-to-use and trusted form of digital identity can contribute to addressing the digital divide by removing some of the technological, confidence and other barriers that can contribute to citizens choosing not to adopt a digital identity, and subsequently missing out on participating in the digital world.

81.2 *ensuring the digital rights of citizens within a trusted online environment;*

Trusted digital identity solutions will also contribute to the development of an online environment in which citizens and businesses have the ability, trust and confidence to take advantage of the opportunities offered by digital technology. Further, access to a trusted form of digital identity is a fundamental element of digital citizenship, together with access to technology and connectivity. These concepts are likely to be addressed within a future digital rights framework.

81.3 *accelerating the growth of the digital economy – making ICT the second largest contributor to GDP by 2025; and*

The Government has stated its intention to take a joined-up, aspirational approach to the digital economy, seeking to increase productivity, drive innovation and economic development, and capitalise on the benefits of the Internet. A strong digital identity system, while not an end in itself, will support the development of the digital economy, offering a reliable, secure, scalable, privacy-enhancing, and convenient identity solution.

81.4 *accelerating digital transformation across the public sector.*

A new digital government strategy is being developed to accelerate digital transformation across the public sector, and set the direction for digital society and the digital economy. A key focus of this initiative involves working with citizens so that public services are designed around their needs. Digital identity is an essential enabler of this programme of activity, supporting citizens to seamlessly manage their digital identity and personal information across multiple domains.

82. In addition, steps will be taken to ensure that work to progress digital identity aligns with the planned modernisation of the Privacy Act 1993, designed to reflect changes in the handling of personal information. Proposed changes include the mandatory reporting of data breaches, steps to enable the Privacy Commissioner to issue compliance notices, and the strengthening of cross-border data flows.

83. At the same time, government has begun work (led by Statistics New Zealand) on the development of a framework for data governance across the public sector, ensuring that it is appropriately managed as an all-of-government asset.

**Alignment with international approaches**

84. The transition team has completed a scan of comparable international jurisdictions (e.g. Australia, Canada and the United Kingdom) to identify the range of approaches to digital identity. It is evident that governments are facing a similar set of drivers for the adoption of universal digital identity solutions as New Zealand, including:
84.1 improved access, effectiveness, efficiency, public service quality and user satisfaction;
84.2 simplification of login procedures for users by providing a single system for login; and
84.3 reducing costs when establishing new secure public services through the standardisation of identity management and login procedures.

85. In each case, work is at an early stage of development. No jurisdiction has yet to resolve the challenges of providing a coherent digital infrastructure. This reflects the complexity of the operating environment, including the need to manage citizen expectations, security requirements and the regulatory environment, alongside technological and information management challenges, and issues of cost and funding. However, there is a willingness to work collaboratively with New Zealand and to create identity standards that will allow cooperation across jurisdictions as far as possible.

86. New Zealand is comparatively well-positioned to resolve issues surrounding digital identity. We have a non-federal and unicameral system of government, a supportive regulatory environment, and a willingness to collaborate across the public and private sectors.

Benefits, risks, constraints and dependencies

Main benefits

87. The following tables summarise the main monetary (Table 1) and non-monetary (Table 2) benefits identified by the transition team in consultation with key stakeholders:

### Table 1: Identified monetary benefits

<table>
<thead>
<tr>
<th>Main benefits</th>
<th>Who benefits?</th>
<th>Direct or indirect?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduced manual verification – Citizens/customers</td>
<td>Citizens/customers</td>
<td>Direct</td>
<td>Reduced costs associated with sourcing and providing physical documents to agencies</td>
</tr>
<tr>
<td>Reduced manual verification – Government</td>
<td>Individual government agencies and the Government as a whole</td>
<td>Direct</td>
<td>Enables a move to fully digital services. The high cost of paper-based identity verification can be replaced with lower cost digital identity verification. Not ‘cashable’ – government agencies will claim benefits as they move to digital channels</td>
</tr>
<tr>
<td>Reduced manual verification – Business and NGOs (includes anti-money laundering requirements)</td>
<td>Private sector and non-government organisations</td>
<td>Direct</td>
<td>The cost of shared digital identity services will be spread across more organisations, resulting in reduced cost per login and attribute assertion</td>
</tr>
<tr>
<td>Main benefits</td>
<td>Who benefits?</td>
<td>Direct or indirect?</td>
<td>Quantitative or qualitative?</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Improved citizen/customer experience and reduced compliance costs</td>
<td>Citizens – through reduced effort for individuals (time and associated costs saved in accessing and supplying physical documentation between multiple agencies)</td>
<td>Direct</td>
<td>Both quantitative and qualitative</td>
</tr>
<tr>
<td></td>
<td>Citizens – through improved satisfaction with identity services</td>
<td>Direct</td>
<td>Qualitative</td>
</tr>
<tr>
<td>Improved equity of access to services</td>
<td>Citizens/ consumers who are disadvantaged by location, capability or concerns about technology use</td>
<td>Direct</td>
<td>Quantitative</td>
</tr>
<tr>
<td>(addressing digital divide)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improved delivery and targeting of government services</td>
<td>Citizens – supports the proactive delivery of entitlements (e.g. superannuation) and ease of access to other supports</td>
<td>Direct</td>
<td>Both quantitative and qualitative</td>
</tr>
<tr>
<td>(esp. free tertiary study and superannuation entitlement)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables growth in the digital economy</td>
<td>Government benefits from economic growth Business benefits from increased opportunities, profitability Citizens benefit from increased opportunities and consumer choice</td>
<td>Direct</td>
<td>Both quantitative and qualitative</td>
</tr>
<tr>
<td>(citizens and business have confidence in the digital marketplace)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improved protection against cyber-threats and privacy invasion</td>
<td>Citizens; small to medium sized businesses and NGOs who can’t afford the protections that government and large businesses can purchase – all benefit thought reduced vulnerability Business and Government – through improved trust in business and government services</td>
<td>Direct</td>
<td>Quantitative</td>
</tr>
<tr>
<td>Costs and risks of digital identity are shared between government and business</td>
<td>Government agencies (and government as a whole), private and NGO sectors</td>
<td>Direct</td>
<td>Both quantitative and qualitative</td>
</tr>
<tr>
<td>(through joint investment in digital identity)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Individuals and organisations can safely and more easily transact on behalf of others</td>
<td>Individuals and organisations who act on behalf of organisations or citizens</td>
<td>Direct</td>
<td>Both quantitative and qualitative</td>
</tr>
</tbody>
</table>
Main risks

88. Investing in digital identity solutions carries several inherent risks associated with changes in technology, in citizen preferences and expectations (especially in relation to trust and confidence), in security and privacy threats, and shifts in the political environment. However, ‘doing nothing’ is not a realistic option.

89. Any shift in the approach of digital identity service provision must be undertaken in a visible and transparent way. It is recommended that the Government has an open dialogue with citizens, communities of interest (including advocacy groups) and business to identify risks and concerns and to co-design aspects of the new approach (particularly related to issues of governance, usability, privacy, trust and security).

90. The transition team has analysed the main risks, as follows (the majority of risks are expressed in terms of the ecosystem option, although many of the demand, supply and delivery risks will apply equally to any option that relies on multiple providers of identity services):

<table>
<thead>
<tr>
<th>Main Risk</th>
<th>Consequence (H/M/L)</th>
<th>Likelihood (H/M/L)</th>
<th>Risk Management Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Political/Stakeholder Risk</strong>&lt;br&gt;(Cross-party sponsorship and commitment)&lt;br&gt;Shifts in the political environment may result in change in approach</td>
<td>Medium (M) – wider participation and investment depends on stable commitment</td>
<td>Medium (M)</td>
<td>• Gain cross-party commitment, where appropriate&lt;br&gt;• Secure stakeholder champions</td>
</tr>
<tr>
<td>Negative public reaction and/or poor understanding of ecosystem causes negative political response and/or poor citizen uptake of services</td>
<td>M – loss in trust and confidence in the ecosystem approach and potential shut down</td>
<td>Low (L)</td>
<td>Open and transparent processes, including:&lt;br&gt;• Putting citizens at the centre&lt;br&gt;• Involving advocacy/interest groups in ecosystem design and parameters&lt;br&gt;• Co-design of trusted identity framework, in partnership with citizens, advocacy/interest groups, business and others&lt;br&gt;• Thorough user-testing processes</td>
</tr>
<tr>
<td>Poor understanding of ecosystem benefits</td>
<td>Low (L) – can create churn, increasing costs and delaying benefits</td>
<td>High (H)</td>
<td>• Co-design of trusted identity framework (as above)&lt;br&gt;• Widespread and early communications and relationship management</td>
</tr>
<tr>
<td><strong>Demand Risks (investment and strategic)</strong>&lt;br&gt;(Take-up by agencies, private companies &amp; NGOs)&lt;br&gt;Insufficient and delayed demand due to high cost of transition or integration</td>
<td>M – reduces value of ecosystem and attractiveness to suppliers, causing reduced citizen/customer choice, lower competition and higher prices</td>
<td>H</td>
<td>• Investment in transition support, integration toolkits&lt;br&gt;• Selection of easy to use and integrated technologies</td>
</tr>
<tr>
<td>Main Risks</td>
<td>Consequence (H/M/L)</td>
<td>Likely hood (H/M/L)</td>
<td>Risk Management Strategies</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Insufficient demand due to risk aversion and poor commitment</td>
<td>M – reduces value of ecosystem and attractiveness to suppliers, causing reduced citizen/customer choice, lower competition and higher prices</td>
<td>M</td>
<td>• Retention and migration of existing RealMe clients&lt;br&gt;• Joint governance with public, private and NGO sectors&lt;br&gt;• Strong leadership and assistance in assessing risks against the government risk framework&lt;br&gt;• Adequate funding of ecosystem development function</td>
</tr>
<tr>
<td>Insufficient demand due to poor match with service requirements (e.g. functions, trust levels)</td>
<td>M – reduces value of ecosystem and attractiveness to suppliers, causing reduced citizen/customer choice, lower competition and higher prices</td>
<td>M</td>
<td>• Comprehensive research into agency, business and NGO requirements&lt;br&gt;• Pipeline prioritisation and design of Minimum Viable Product to meet majority of pipeline requirements</td>
</tr>
<tr>
<td>Demand is split because existing identity services are not incorporated into the new shared ecosystem, and service providers are not transitioned</td>
<td>M – reduces value of ecosystem and attractiveness to suppliers, causing reduced citizen/customer choice, lower competition and higher prices</td>
<td>M</td>
<td>• Clear governance that includes all current identity services and service providers using current services&lt;br&gt;• A clear mandate that government services are to use identity services from a new shared identity ecosystem</td>
</tr>
</tbody>
</table>

**Supply Risks (investment and strategic)**

(too few identity providers or offerings)

| Insufficient supply due to high barriers to ecosystem entry or exit – e.g. over-regulation, costly accreditation or procurement | M – causes reduced citizen/customer choice, lower competition and higher prices | M                   | • Co-design and close engagement with public and private sectors |
| Insufficient supply due to risk aversion and/or lack of investment capital | M – causes reduced citizen/customer choice, lower competition and higher prices | L                   | • Create value that ecosystem can deliver to identity suppliers (e.g. identity information for banks)<br>• Capital investment underwriting<br>• Capital investment funds |
| Insufficient supply due to ecosystem size and value being small | M – causes reduced citizen/customer choice, lower competition and higher prices | M                   | • Stimulate early demand through incentives or penalties<br>• Government guaranteed revenue (subsidy) |

**Delivery Risks**

<p>| Over-regulation stifles ecosystem viability | M – could cause ecosystem to fail | M                   | • Establish multi-stakeholder engagement and input early in ecosystem design phase |
| Technical or operational failure | High (H) – government digital services would be inaccessible | L                   | • Design high levels of redundancy and availability into the market exchange mechanisms |</p>
<table>
<thead>
<tr>
<th>Main Risks</th>
<th>Consequence (H/M/L)</th>
<th>Likely hood (H/M/L)</th>
<th>Risk Management Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ecosystem does not meet requirements of citizens, customers, government,</td>
<td>M — could create supply or demand risks and reduce uptake, could prevent realisation</td>
<td>L</td>
<td>• Engage widely with stakeholders during market design</td>
</tr>
<tr>
<td>suppliers or digital service providers</td>
<td>of strategic goals of government</td>
<td></td>
<td>• Co-design and close liaison with public, private and NGO sectors</td>
</tr>
<tr>
<td>Ecosystem is not agile or flexible enough to keep up with requirements of</td>
<td>M — would affect long term viability and sustainability of ecosystem, and ultimate</td>
<td>M</td>
<td>• Design ecosystem to maximum competition</td>
</tr>
<tr>
<td>citizens, customers, government, suppliers or digital service providers</td>
<td>return on investment</td>
<td></td>
<td>• Lean Start-up Design principles and methodology, followed by ecosystem development delivery provider</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Build innovation programmes into ecosystem development function and funding</td>
</tr>
<tr>
<td><strong>Reputation and Trust Risks</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ecosystem security or privacy is breached</td>
<td>H — loss of trust in government services by citizens and business</td>
<td>L</td>
<td>• Highest level of Privacy and Security designed into the ecosystem mechanisms (Privacy and Security by Design)</td>
</tr>
</tbody>
</table>

**Key constraints and dependencies**

91. The proposal is subject to the following constraints and dependencies. These dependencies will be carefully monitored during the project.

**Table 4: Constraints and dependencies**

<table>
<thead>
<tr>
<th>Constraints</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Act 1993</td>
<td>Privacy principles are embedded as a core component of the project requirements and proposed options will comply with the Privacy Act. The transition team will keep abreast of the planned modernisation of the Privacy Act.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dependencies</th>
<th>Notes and Management Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independent transition team resourced to facilitate the next phase of work</td>
<td>An independent transition team has carried out the work to date, as the key skills needed to develop a collaborative ecosystem do not exist in DIA. A stewardship path reflecting multiple stakeholder interests will be used.</td>
</tr>
<tr>
<td>The willingness of banks and other identity providers to deliver services to the ecosystem</td>
<td>Banks and other potential identity service providers will be key stakeholders and have a voice in stewardship of the design and establishment phase</td>
</tr>
<tr>
<td>The ability of government agencies to provide attributes into the ecosystem</td>
<td>DIA, through the Te Ara Manaaki programme, is creating the capability to provide attributes to the ecosystem. MBIE (Immigration) and Inland Revenue are in the process of developing Application Programming Interfaces related to visa status and income respectively. To be able to move away from paper identity verification other government agencies will need to be able to provide additional attributes.</td>
</tr>
</tbody>
</table>
92. The transition team has been working collaboratively with a range of government agencies to identify project interdependencies with related initiatives (e.g. Ministry of Social Development’s Simplification programme; Oranga Tamariki’s Children’s Action Plan; Inland Revenue’s Business Transformation Programme; and the health sector’s Health Identity Programme).

93. Agencies with a significant stake in identity management will continue to be engaged in the next phase of the project as solutions are designed and developed.
Economic case for change

Problem definition

94. The current approach to digital identity is incoherent with inconsistent standards across both the public and private sectors. This is restricting agencies and private sector enterprises in their ability to deliver safe, privacy protected, and efficient digital experiences, while citizens are impacted with high risk, inconvenience and uncertainty. A detailed statement of the problems with the status quo is set out in the Strategic Case.

95. Digital identity is a complex, rapidly changing space involving a wide range of stakeholders with varying identity needs. The Government currently provides digital identity products and services for customers accessing government services through RealMe, but the problems with RealMe are multiple, and vary depending on which lens is taken (citizen, agencies, or private sector).

96. The Government has an opportunity to review its position as the designer, builder, funder and administrator of digital identity solutions, in the context of a vastly different operating environment. The Economic Case sets out a range of potential options for moving forward and assesses these against a range of criteria, including relative costs and benefits.

Critical success factors

97. The following critical success factors were discussed and adapted by stakeholders at the facilitated options workshop held on 10 August 2017:

<table>
<thead>
<tr>
<th>General Critical Success Factors</th>
<th>Broad Description</th>
<th>Proposal specific Critical Success Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic fit and business needs</td>
<td>How well the option meets the agreed investment objectives, related business needs and service requirements, and integrates with other strategies, programmes and projects.</td>
<td>Does the option meet the five investment objectives (listed below)? Does the option align with government strategies, in particular the drive for a “customer-centric, flexible, sustainable ecosystem engaged with private sector”?</td>
</tr>
<tr>
<td>Potential value for money</td>
<td>How well the option optimises value for money (i.e. the optimal mix of potential benefits, costs and risks).</td>
<td>Will identity services provided by the private sector cost less for comparable quality and functionality? Will the benefits outweigh the costs and risks?</td>
</tr>
<tr>
<td>Supplier capacity and capability</td>
<td>How well the option matches the ability of potential suppliers to deliver the required services, and is likely to result in a sustainable arrangement that optimises value for money.</td>
<td>Will enough suppliers of identity services and customers of identity services be attracted to the market?</td>
</tr>
<tr>
<td>General Critical Success Factors</td>
<td>Broad Description</td>
<td>Proposal specific Critical Success Factors</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Potential affordability</td>
<td>How well the option can be met from likely available funding, and matches other funding constraints.</td>
<td>Can the option be funded within existing baselines and/or new revenue sources? Is the option the lowest cost to government?</td>
</tr>
<tr>
<td>Potential achievability</td>
<td>How well the option is likely to be delivered given the organisations ability to respond to the changes required, and matches the level of available skills required for successful delivery.</td>
<td>Can the option feasibly be delivered, and can suppliers and customers of identity services feasibly take up the market services?</td>
</tr>
</tbody>
</table>

98. The five investment objectives established for this programme include:

98.1 Meets trust and privacy requirements
98.2 Designed from a citizen perspective and improves equity of access
98.3 Delivers productivity gains
98.4 Provides best value for investment and shares risk
98.5 Future proofing and flexibility.

Long-List options and initial assessment

99. The following long-list options were developed by the transition team and agencies have been consulted. Options are grouped around the role that government plays.

Appendix IV provides a tabular summary of the delivery dimensions of each option. Timeframes are relative and indicative without planning detail.

Government Exits

A Exit all-of-government digital identity
1. R2.4(i)(iv)
2. Each government agency develops and operates its own digital identity system arrangements.
3. While government may issue guidelines, this option is in effect moving to an unstructured and unregulated Digital Identity Ecosystem without agreed standards or clear roles.
Government as a service provider

B Status quo
4. Although RealMe is mandated for government for all levels of identity verification, it is over-engineered and difficult to use for levels 1 – 3. As a result, some agencies adopt other identity verification arrangements for levels 1 – 3.
5. Under the Status Quo:
   • The functionality and ease of use of RealMe for all levels remains unchanged\textsuperscript{12}
   • Government and private sector digital identity services continue to develop separately\textsuperscript{13}.

C Develop RealMe
6. RealMe is mandated for government for all levels of identity verification. Additional and ongoing investment improves functionality and ease of use in RealMe for levels 1 – 4.
7. While government and private sector digital identity services continue to develop separately, the improvements in functionality increase the use of RealMe by private companies to meet their legal responsibilities to comply with the Anti-Money Laundering and Countering the Financing of Terrorism Act 2009.

D Divest login, Develop RealMe IVS
8. Login is fully divested to a number of private providers (such as Trade Me, banks) over a 5-year transition period, at which point the RealMe login service will be discontinued. Private login providers link their logins to RealMe IVS attributes depending on the level of verification required.
9. Development of RealMe improves functionality and ease of use at all levels of verification. RealMe IVS continues and is mandatory for government agencies as in Option C.

\textsuperscript{12} In practical terms, the utility of RealMe is likely to reduce given changes in the wider digital identity environment.
\textsuperscript{13} There already are a few private sector agencies using RealMe, but at insignificant levels.
Collaborative model – joint service provision

E Collaborative Digital Identity Ecosystem

10. Under the Collaborative Digital Identity Ecosystem:

- RealMe IVS continues to be owned and operated by government until this is replaced by alternative service(s) in year 6. RealMe IVS is mandatory for level 4 for government agencies in years 1 – 5, and also used by the private sector.

- Government and private sector digital identity services develop a NZ Inc. digital ecosystem on a collaborative basis, choosing a mix of public and private service providers on a "best-of-breed" basis. Digital identity services are collaboratively developed by customers, agencies and relevant private sector organisations.

- Government may decide to retain delivery of some digital identity components or services for political or security reasons.

- A full digital ecosystem is governed by government and private sector arrangements that cover all levels of verification. Government has a regulatory and standard-setting role in the digital ecosystem across the public and private sectors (a broader role than for Option D).

Government as regulator and standard setter only

F Digital Identity Ecosystem

11. Under a Digital Identity Ecosystem:

- RealMe is phased out as soon as possible.

- Login and identity verification services for levels 1 – 4 are delivered by private sector providers only. Government and private sector develop a NZ Inc. digital ecosystem together.

- Customers, agencies and relevant private sector organisations would collaboratively design the market environment.

- Government has a regulatory and standard-setting role in digital identity across the public and private sectors.

Assessment of Long-List options

100. The long-list options were assessed against the investment objectives and other critical success factors. Each option was scored on a scale of 0 to 5 where:

- 0 = no match to assessment criteria
- 5 = high match to assessment criteria

The assessment is summarised in the table below (a detailed analysis of the options is provided in Appendix V).
## Table 6: Assessment of Long-List options

<table>
<thead>
<tr>
<th>Strategic choices</th>
<th>Exit</th>
<th>Government as service provider</th>
<th>Collaborative model</th>
<th>Government as regulator and standard-setter only</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A. Exit all-of-government digital identity</td>
<td>B. Status Quo</td>
<td>C. Develop RealMe</td>
<td>D. Divest Login / Develop RealMe IVS to continue</td>
</tr>
<tr>
<td></td>
<td>Government provided</td>
<td>Government/Private sector provided</td>
<td>Private Sector Provided</td>
<td></td>
</tr>
<tr>
<td>Investment Objectives</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meets trust and privacy requirements</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Designed from a citizen perspective and improves equity of access</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Delivers productivity gains</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Provides best value for investment and shares risk</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Future proofing and flexibility</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Other Critical Success Factors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic fit and business needs</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Potential value for money</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Supplier capacity and capability</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Potential affordability</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Potential achievability</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Total Score</td>
<td>13</td>
<td>16</td>
<td>28</td>
<td>36</td>
</tr>
<tr>
<td>Overall Assessment</td>
<td>Reject: low alignment to assessment criteria. Not credible.</td>
<td>Carry forward to short-list</td>
<td>Carry forward to short-list: high match to criteria</td>
<td>Carry forward to short-list: highest match to criteria</td>
</tr>
</tbody>
</table>
Recommended strategic direction

101. The preferred approach is to establish a collaborative digital identity ecosystem (Option E). This option is likely to have the highest ratio of benefits to costs. It is also the only option that:

101.1 provides a single digital identity system on a New Zealand-wide basis that maximises digital inclusion by enabling citizens to operate seamlessly between the public and private sectors;

101.2 enables economic growth and productivity gains through providing citizens, government and the private sector with confidence to interact and transact online through the use of familiar, accessible and trusted systems; and

101.3 reduces overall costs by moving from existing arrangements onto more cost-effective arrangements which utilise the best of public and private sector systems, expertise and capabilities.

102. The digital identity ecosystem (illustrated in Figure 4 below) will function as a cohesive but flexible constellation of loosely connected solutions from multiple parties that combine to deliver value to end users. Parties would include those that provide data attributes or package these as identity services (such as RealMe IVS), those that address login, and those that rely on providers in order to deliver end user value. Coherence in the system is achieved through infrastructural standards in process and technology and through adherence and operation under the rules of the Digital Identity Trust Framework.

**Figure 4: NZ Digital Identity Ecosystem**

- Governance, management and operations – functions to ensure the smooth running of the ecosystem
- Digital Identity Trust Framework – sets the rules, parameters and monitoring arrangements for the ecosystem
- Solution space – allows multiple providers to transact with multiple relying parties (maintains security and privacy requirements)

Agencies and private sector organisations can undertake multiple roles in the ecosystem

Funding from multiple sources
103. While Option E is distinct from other options assessed here, it is a strategic direction within which there remain numerous variables and dynamic externalities. It is unclear as yet what the optimum ecosystem design should be. It will involve balancing, for example, scope of services, degree of technical investment and operational involvement by the private sector, speed of development by vendors, impact of international trends, and degree of control required in governance and operation by government. The process of collaboration itself will give clarity to the exact nature of government intervention as the ecosystem evolves.

104. For these reasons a more agile and iterative approach is required, with appropriate checks and balances. The traditional, indicative and then detailed business case approach assumes the preferred option can be articulated with sufficient clarity and foresight to quantify costs and benefits. In the case of the digital identity ecosystem and its emerging solution set and dynamic environment, this picture is still materialising and will indeed be co-designed with other participants.

105. The approach will follow a set of controlling principles for the work programme:

105.1 **Open and transparent** – with investigations, assessments and recommendations available for input by ecosystem participants;

105.2 **Consultative co-design** – actively seeking input from participants;

105.3 **Citizen centric** – using system thinking to design the ecosystem around user needs;

105.4 **Agile iterative** – progressing in steps – “learn fast” with decision points to enable continuation, change of direction, or further research/work/consultation to inform the next phase of the initiative; and

105.5 **Technology agnostic** – working without predetermined or preferred technologies.

106. The ecosystem environment will also aim to represent principles developed in collaboration with participants, such as:

106.1 **Choice and control** – Users have choice and control over how they interact with service providers and share their data. Users have full ownership of their data with consent-based attribute sharing. Users are able to delegate responsibility to others to act in different roles;

106.2 **Standards and rules compliance** – Compliance with AML, Privacy and the European Union General Data Protection Regulation. Address security and privacy concerns regarding authentication and access to data. Adherence to a common digital identity trust framework;

106.3 **Openness and transparency** – Support both central and/ or distributed solutions. Open marketplace of loosely coupled components (engaged via clear contracts). Open standards and open source of reference implementation;

106.4 **Interoperability** – across technology types, service providers and other jurisdictions;
106.5 **Sustainable ecosystem** – Environment that encourages open competition and participation. Affordable and cheap to adopt for organisations and users. Digital Inclusion – ensuring disadvantaged groups have access to and skills to use ICT, enabling participation in society;

106.6 **Ease of use** – for both users and organisations; and

106.7 **Cross domain usage** – Private and public sector, large and small organisations, degree of regulation.

**Next steps**

107. This Feasibility Study seeks confirmation of the viability of the collaborative digital identity ecosystem concept and approval for the transition team to continue to work with the private sector and government agencies to build and test aspects of the collaborative digital identity ecosystem.

108. Proposed key activities over the next 24 months include:

108.1 **Governance** framework to confirm work programme detail. Independent Advisory Group facilitation, and reporting to Ministers.

108.2 **Policy Development** to work alongside citizens and the private and non-government sectors to design a Digital Identity Trust Framework that sets the ‘rules of the game’ for the new approach, including protection of the privacy and security interests of citizens. This will also provide context for a regulatory review.

108.3 **Operating Model Options** using user-centric service design approaches to test concepts and prototype improvements to digital identity infrastructure. This will inform recommendations regarding future operating models and architectures.

108.4 **Engagement and Transition**, including input to the RealMe strategy, change management and stakeholder transition planning, bringing the public and private sectors together and consulting citizens.

109. The detailed work programme that will be formed to deliver these activities will ensure clear traceability between its outputs, the changes enabled, outcomes realised, benefits achieved and the overall programme objectives. A draft value map to draw these linkages is attached as **Appendix VI**.
### Appendix I: Key stakeholders engaged

**Other jurisdictions:**
- **Canada**
  - DIACC
  - SecureKey
  - Canada Government
- **Republic of Ireland**
- **Finland**
- **Sweden**
- **Norway**
- **United Kingdom**
  - UK Verify
  - Wider UK Government
- **Australia**
  - Digital Transformation Agency
  - Queensland Government
  - Wider Australian Government

**Within New Zealand (illustrated below)**

#### Public Sector
- Accident Compensation Corporation
- Auckland City Council
- Auckland District Health Board
- Department of Corrections
- Department of Internal Affairs
- Electoral Commission
- Government Communications Security Bureau
- Inland Revenue
- Land Information New Zealand
- Ministry of Business, Innovation and Employment
- Ministry for Children – Oranga Tamariki
- Ministry of Education
- Ministry of Health
- Ministry of Justice
- Ministry for Primary Industries
- Ministry of Social Development
- National Cyber Policy Office
- New Zealand Customs Service
- New Zealand Transport Agency
- Office of the Privacy Commissioner
- State Services Commission
- Statistics New Zealand
- Te Puni Kōkiri
- The Treasury
- Wellington City Council

#### Private Sector
- Accenture
- ASB
- BNZ
- Centrality
- Daon
- Datacom
- Data Zoo
- Forrester
- Forsyth Barr
- Gartner
- GreenID/PIM
- IAG
- InternetNZ
- Keyp
- Kiwibank
- Mercury
- Minter Ellison
- Microsoft
- NZ Bankers Assoc.
- NZRise
- NZTech
- Origin IDANZ
- IBM
- Paymark
- Origin IDANZ
- IBM
- Paymark
- Payments NZ
- Ping ID
- Privacy Foundation
- Spark/Qrious
- Tuakiri
- Trade Me
- Veda/Equifax
- Vodafone
- Westpac
- Xero
Appendix II: Sample global research

A sample of global research articles on the importance of digital identity

Australia Post

Boston Consulting Group/Liberty Global

Deloitte

The Economist
   • http://www.eiuperspectives.economist.com/technology-innovation/economics-digital-identity

World Bank

World Economic Forum
   • http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf
Appendix III: Provider Market Scan

An indicative list of vendors involved in digital identity

New Zealand based:

Existing
- 2 Shakes
- Centrix
- Data Zoo
- Infolog
- OriginID
- Verifi/Cloudcheck

Emerging
- EGO
- Kauri

Multinationals with New Zealand presence:

Existing
- Acuant
- Bitium
- Civic ID
- Daon
- Equifax
- Experian
- EZMCOM
- Forgerock
- Green ID/VixVerify
- Hypr
- Jumio
- LelixNexis Risk Solution
- OIX
- SimpleKYC
- Trusona
- Whitepages pro

Emerging
- Sphere Identity
- Sovrin
- Keyp

Generic
- Alphabet
- Microsoft

Vendors without current New Zealand presence:

Existing
- AU10TIX
- Australia Post
- Datavisor
- Direct ID
- DUO
- Evernym
- ID Analytics
- IdentityMind
- IDology
- Kount
- Mitek
- PinDrop
- REALFACE
- SecureKey
- TransUnion
- Trulioo
- Yubico

Emerging
- AuthO
- Bitfury
- Confirm IO
- CryptID
- Tierion
- Onfido
- Rivetz
- Shape
- ShoCard
- Tradle
- Tykn
- VelixID
- VeryMe
# Appendix IV: Delivery Dimensions for Long-List Options

<table>
<thead>
<tr>
<th>What is the role of government in digital identity?</th>
<th>EXIT</th>
<th>Government as SERVICE PROVIDER</th>
<th>COLLABORATIVE model – joint service provision</th>
<th>Government as REGULATOR and STANDARD-SETTER only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>A. Exit all-of-government digital identity</td>
<td>B. Status Quo</td>
<td>C. Develop RealMe</td>
<td>D. Divest Login / Develop RealMe IVS to continue</td>
</tr>
<tr>
<td>Service providers</td>
<td>Government/Private Sector Provided</td>
<td>Government Provided</td>
<td>Government / Private Sector Provided</td>
<td>Government / Private Sector Provided</td>
</tr>
<tr>
<td>Government agencies</td>
<td>Up to individual government agencies</td>
<td>Government</td>
<td>Government</td>
<td>Primarily government</td>
</tr>
<tr>
<td>Scope of digital identity</td>
<td>Government</td>
<td>Government</td>
<td>Government</td>
<td>Primarily government</td>
</tr>
<tr>
<td>RealMe continues as Service Solution:</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (apart from Login)</td>
</tr>
<tr>
<td>Governance</td>
<td>Individual government agencies</td>
<td>Government only</td>
<td>Government only</td>
<td>Government only</td>
</tr>
</tbody>
</table>

---

14 No all-of-government digital identity service.

15 Government’s role is regulator and standards-setter only.
Appendix V: Assessment of Long-List Options

A. Exit all-of-government digital identity

Advantages
- Opens opportunities for the private sector to innovate and provide services to government. Government guidelines (rather than standards) may provide agencies with greater flexibility.

Disadvantages
- Makes delivery and targeting of government services (particularly to high users or those with complex needs) more difficult.
- No coordination of investment, and duplication of services, increases cost across government.
- Lack of standards, coordination and integration across government:
  - reduces digital inclusion;\(^{16}\) and
  - degrades the user experience and increases the risk of fraud and privacy breaches.
- Fragmented design and delivery may compromise the quality of digital identity verification.
- Gaps/ loss of level 4 service continuity for agencies that currently rely on RealMe is critical.
- Costs and implementation risks are concentrated within individual agencies, and may not be transparent.
- No integration with the private sector means opportunities to improve services and reduce costs across the digital identity market are missed.

Conclusion
Not a viable option. Closing down RealMe before a viable alternative is available:
- is likely to be unacceptable from the perspective of citizens and agencies (reduce digital inclusion and increase the cost and risk of government service delivery);
- would leave government agencies to develop stand-alone systems within a limited timeframe, and loss of service continuity could be crippling for some agencies;
- will constrain efforts to improve digital inclusion;
- is likely to make delivery of existing services and new services (such as delivery of free tertiary fees) more difficult;
- will increase costs of service delivery across government;
- is likely to increase the risk of identity fraud and privacy breaches in government services; and
- would signal the New Zealand Government has limited interest in digital identity and improving government service delivery. This may impact on New Zealand’s international reputation.

---

\(^{16}\) The ability of individuals and groups to access and use information and communication technologies
B. Status Quo

Advantages

- A product set with known issues.
- Centralised design, delivery and reduced duplication of services provides an opportunity to:
  - improve the overall quality of digital identity verification and consistently meet minimum standards; and
  - reduce costs across government.
- Government maintains a high degree of control over service delivery, providing greater confidence around the use of customer data.

Disadvantages

- Costly, relies on outdated architecture and difficult to use for levels 1-3 (it is designed for level 4 identity verification).
- Does not meet current (let alone future) business needs.
- Does not address the limitations of RealMe as the single all-of-government option for levels 1-4 as described in independent reviews.
- New funding will be required for the development of RealMe in 2018/19 and outyears.
- No development of levels 1-3 functionality means little improvement in the user experience. As a result, many agencies work around RealMe and/ or develop alternative arrangements for levels 1-3. Cost and difficulty to use constrains the development of government service delivery for levels 1-3.
- Gaps in RealMe and negative perceptions held by users and government agencies would need to be overcome for this option to be sustainable.
- Ongoing development costs and implementation risks are high, concentrated within government. Development is expected to require significant ongoing investment.
- No integration with private sector means opportunities to improve services and reduce costs across the identity market are missed. Cannot deliver economic and productivity gains to NZ Inc.
- No opportunities for the private sector to provide services to government.

Conclusion
C. Develop RealMe further

**Advantages**
- Improves delivery and targeting (such as superannuation and free tertiary study) of government services (particularly to high users or those with complex needs).
- Coordination and integration of services across agencies improves the user experience.
- Centralised design and delivery should improve the quality of digital identity verification.
- Supports efforts to improve digital inclusion.
- Supports integration of services across government (particularly for high users of government services).
- While funding for RealMe will need to increase, reduced duplication of services should reduce overall digital identity costs to government.
- Government maintains a high degree of control over service delivery, providing greater confidence around the use of customer data.

**Disadvantages**
- Significant new funding required on an ongoing basis for development and maintenance of RealMe.
- Overcoming negative perceptions of RealMe by citizens and government agencies to the point where this option is sustainable would be a significant challenge.
- No integration with private sector means opportunities to leverage off existing private sector services in order to improve services and reduce costs are missed.
- Does not deliver economic and productivity gains to NZ Inc.
- Opportunities for the private sector to provide services to government may be limited.
- Limited use of RealMe to meet AML compliance requirements.

**Conclusion**
A potentially viable option.

D. Divest login / Develop RealMe IVS to continue

**Advantages**
This option has the same advantages as Option C (Develop RealMe), plus:
- As users will use familiar logins that they use regularly to access government services, this will:
  - improve user satisfaction;
  - improve equity of access to services;
  - improve digital inclusion; and
  - reduce agency operating costs through reducing the number of login resets required.
- Allows agencies and users a choice of login provider for level 1-3 services.
Logins will link to different RealMe IVS attributes, depending on the level of verification required. This flexibility will enable different logins to be developed for levels 1-3.

Agencies are directly charged for logins by private providers.

RealMe Login costs can be removed in year 6 and outyears.

Disadvantages
This option has the same disadvantages as Option C (Develop RealMe), plus:

- Significant new funding required for development and maintenance of RealMe in 2018/19 and outyears;
- Transition costs to:
  - link RealMe IVS attributes to private sector login providers for levels 1-3; and
  - modify user agency systems to operate with a number of private login providers.
- Exit costs in year 6 for any redundancy or asset write-offs required as a result of closing down the RealMe Login service;
- Opportunities to leverage existing private sector services, and share costs and investment risks are limited to login only; and
- Limited use of RealMe to comply with AML regulations.

Conclusion
A potentially viable option.

E. Collaborative Digital Identity Ecosystem

Advantages

- A well-managed digital ecosystem will contribute to:
  - making it easy for New Zealanders to manage their online activities seamlessly across the government and private sector;
  - improve digital inclusion by providing New Zealanders with easier and more equitable access to services, including a reduction in effort when interacting with government;
  - enabling the efficient and effective delivery of public services by reducing the costs of transactions and supporting the proactive delivery of entitlements such as national superannuation and free tertiary education;
  - supporting the use of digital engagement tools to transform democratic processes, including participation in public policy development processes and, ultimately, e-voting;
  - open data initiatives, by providing agencies with assurance that an individual requesting they share their data is who they say they are; and
  - supporting private sector innovation and efforts to improve productivity and competitiveness, and to comply with AML regulations.

---

17 Estimated to be approximately 66% of total RealMe operating costs.
18 A structured, regulated ecosystem with agreed standards and clear roles.
• Market-focused and centralised design and delivery should improve the quality of digital identity verification.
• Allows agencies and users a choice of provider for all levels (after Year 5).
• Reduced duplication of services should reduce costs across government and the digital identity market.
• Government maintains control over level 4 verification (which is critical and high risk for some agencies) with a managed transition onto a new system in Year 5.
• Innovative solutions are more likely to be introduced and over time competition may produce higher quality and more efficient services.
• Agencies providing identity verification services to private sector groups may be able to recover costs by charging for services.
• Government benefits from sharing investment and implementation risks with the private sector.
• Likely to lead to more sustainable and flexible digital identity services than continued government ownership and operation.
• Government benefits from private sector innovation. Focusing government investment on market facilitation and regulation is likely to be a more efficient and effective use of government resources.
• Phase out of RealMe addresses negative perceptions of government provision of verification services.
• Enables AML regulations to be complied with. Companies that deal with funds and transact on behalf of others are required to verify the identity of clients (to ensure clients are who they say they are). This includes existing clients as well as new ones.

**Disadvantages**

• Facilitating an effective market would require additional ongoing cost (e.g. for regulation and enforcement of standards).
• Government has less control over level 4 verification (after Year 5), which raises risks around quality of this critical verification level which will need to be managed.
• Cannot be implemented before an alternative other than RealMe for level 4 verification is available in the NZ market.

**Conclusion**

The most viable approach.

---

19 Such as banks, Kiwisaver providers, solicitors, real estate agents.
F. Digital Identity Ecosystem

Advantages

This option has the same generic advantages of a well-managed digital ecosystem outlined in Option E (Collaborative Digital Identity Ecosystem) above, plus:

- Coordination and integration of services across agencies and the private sector significantly improves the user experience;
- Centralised design and delivery should improve the quality of digital identity verification;
- Enables government to focus on regulatory and standard-setting roles;
- Allows agencies and users a choice of provider for all verification levels;
- Reduced costs to government (although Private Sector providers may not necessarily be lower cost);
  Innovative solutions are more likely to be introduced and over time competition may produce higher quality and more efficient services;
- Agencies providing identity verification services to private sector groups may be able to recover costs by charging for services;
- Government benefits from private sector investment. Focusing government investment on market facilitation and regulation is likely to be a more efficient and effective use of government resources;
- Phase out of RealMe addresses negative perceptions of government provision of identity verification services; and
- Improved integrity of systems such as banking information and payment engines (e.g. those used by MSD and IR).

Disadvantages

- Private Sector providers may not meet the needs of Government agencies.
- Government does not maintain control over level 4 verification. This raises risks around quality of this critical verification level that will need to be managed.
- May result in increased cost (i.e. private sector providers may not necessarily provide services at lower cost than government agencies).
- Facilitating an effective market would require additional ongoing cost (e.g. for regulation and enforcement of standards).
- Cannot be implemented before an alternative to RealMe for level 4 verification is available in the New Zealand market.

Conclusion

Not a viable option at this time. It is not considered possible to move directly to a market-only model (with Government being a regulator and standard setter only) at this stage without first adopting a market-focused ecosystem model. Implementation of this option is therefore considered to be high risk at this time. This position is likely to change as the market matures and new technologies become more established.