Chair  
Cabinet Economic Growth and Infrastructure Committee  

REGULATIONS AND OTHER ISSUES TO SUPPORT THE ELECTRONIC IDENTITY VERIFICATION BILL  

Proposal  
1 This paper seeks Cabinet’s agreement to:  

- issue drafting instructions for the development of regulations to support the implementation of the Electronic Identity Verification Bill (the Bill), once enacted; and  
- provide joint Ministers with the authority to make necessary changes to the Identity Verification Code of Practice 2011 under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the AML/CFT Act).  

Executive summary  
2 The Bill establishes the identity verification service (the Service) which allows individuals to prove who they are online. Use of the Service will enable more secure government and private sector services to be made available online.  

3 The Bill requires regulations to declare agencies to be “participating agencies” that are authorised to use the Service to verify individuals’ identities. This can be done by listing classes of agencies or by listing individual agencies. I am seeking decisions about the contents of regulations now, in order to bring the Bill into force as soon as possible after it is enacted.  

4 I propose that regulations make the Service available to all agencies within the wider public sector (including Public Service and non-Public Service departments, Crown entities, State-owned enterprises and local government).  

5 For private sector agencies, I propose that Cabinet agree to a policy framework based on four basic principles (necessity, trust, alternative service delivery and usability) for considering which agencies could use the Service. As registered banks meet the policy framework, the regulations will declare that they be a class of participating agencies.  

6 The remainder of the regulations are largely administrative and cover the duration of electronic credentials, the period that credential information can be retained and declare that three agencies may provide identity information checks.  

7 In addition, I am seeking agreement to make necessary changes to the Identity Verification Code of Practice 2011 under the AML/CFT Act once the Bill is
enacted to ensure that the requirements of the AML/CFT Act are met by the Service.

**Background**

8 The Bill was introduced into Parliament on 30 August 2011. The Government Administration Committee considered the Bill and reported back on 19 June 2012 and the Bill passed its second reading on 29 August 2012. The Bill has a priority of 2 on the 2012 legislation programme, and is awaiting consideration by the committee of the whole House.

9 The Bill governs the operation of the Service. The Service enables individuals to prove who they are online in a secure manner which protects privacy. Individuals consent to their information being shared with participating agencies with which they wish to transact. The information that is shared, through electronic identity credentials (credentials), comprises only the individual’s name, sex, date of birth and place of birth. One of the core premises of the Bill is that individuals are in control of their information.

10 The Service will be an important tool to support the Government’s actions to achieve Better Public Services Result 10 (New Zealanders can complete their transactions with the Government easily in a digital environment). Use of the Service will enable more Government transactions to be offered online, particularly those where the agency offering the transaction needs to be confident about the identity of their customers.

**Policy decisions on regulations**

11 The Bill provides for a wide range of regulation-making powers. Although the Bill is still before the House, I propose that Cabinet make decisions on these regulations at this time in order to allow the Bill to be brought into force as soon as possible once enacted.

**Participating agencies**

12 The Bill requires regulations to declare agencies to be “participating agencies”. Only participating agencies are authorised to use the Service to verify individuals’ identities where required for the services they offer. This can be done by listing classes of agencies or by listing individual agencies.

**Public sector**

13 I propose that regulations authorise all public sector agencies to use the Service. It is appropriate to make the Service available to all agencies within the wider public sector (including Public Service and non-Public Service departments, Crown entities, State-owned enterprises and local government) as:

- Cabinet has recently directed chief executives of departments to use the igovt services [CAB Min (12) 23/12]. This Cabinet decision strengthens previous Cabinet decisions relating to the igovt services for departments [CAB Min (08) 38/2A and CAB Min (10) 35/5A];
In 2008, the then Ministers of Finance and State Services issued a whole of government direction about the igovt services, to control the investment or building of separate online establishment and verification capability by all Crown agents;¹ and

Other public sector agencies (including local government and council-controlled organisations) are also encouraged to use the igovt services, and several are already using the igovt logon service.

**Private sector**

14 I propose that Cabinet agree to a policy framework for considering which private sector agencies could be participating agencies. The policy framework is set out in Appendix A. The four basic principles of the framework are:

1. *Necessity* – the agency must have a legitimate need to use the Service;
2. *Trust* – the agency must be trustworthy, can demonstrate compliance with relevant legislation and be stable;
3. *Alternative service delivery* – the agency must provide alternative means for customers to verify their identities (when required to do so) so far as is practicable in the circumstances; and
4. *Usability* – the agency must be technically and practically able to use the Service.

15 I propose that the policy framework be agreed by Cabinet to streamline future decision-making about participating agencies. In future, I would recommend to the Governor-General directly (via the Cabinet Legislation Committee and Cabinet) that agencies that meet the approved policy framework be added to the list of participating agencies. This would avoid the need to seek further policy decisions about each new agency or class of agency.

16 At this time, I propose that registered banks be declared as a class of participating agencies. I believe it is appropriate to do so as registered banks meet the policy framework. Registered banks will be subject to the customer due diligence requirements of the AML/CFT Act (*necessity*). They are highly regulated, including requiring the Reserve Bank’s approval to enter the market (*trust*). Most banks offering services to individuals have both online and offline services (*alternative service delivery*). Finally, banks have the technical capabilities to offer online services and deal with a large number of New Zealand-based individuals (*usability*).

17 New Zealand Post Limited and officials will work to identify other private sector agencies seeking to use the Service. I anticipate that these will include utility companies, financial institutions and other agencies subject to the AML/CFT Act. It was recognised that the partnering arrangement with NZ Post could drive the development of new online services and uptake by private sector agencies which, in turn, would stimulate the integration of further services, user uptake

and transaction volume. Full cost recovery will be achieved more rapidly, and this will reduce the overall requirement for Crown revenue funding.

**Fees and charges**

18 The Service’s success will rely on the Service achieving full cost recovery over time. The Bill allows for fees and charges to recover costs from both participating agencies and from individuals using the Service.

**Participating agencies**

19 The Bill allows fees and charges for participating agencies to be set either by regulation or by agreements between the Chief Executive of the Department of Internal Affairs (the Department) and participating agencies. In addition, New Zealand Post Limited, in its partnering role, is empowered to set and collect charges (that may include a profit margin) from the private sector agencies that will use the Service.

20 Setting charges by agreement is appropriate during the start-up phase of the Service. Setting charges through agreements allows a flexible case-by-case approach which is important to support the initial participating agencies’ use of the Service. These charges can only recover the Department’s costs associated with the Service. I therefore propose that, at this stage, there be no prescribed fees for participating agencies and that charges be set by agreements.

21 The agreement approach may be sustainable for many years. However, it may be necessary to prescribe fees if concerns are raised by agencies, or if additional transparency is required. Prescribed fees would also be required if decisions were made for fees to apply to individuals using the Service.

**Individuals**

22 The Bill also allows individuals to be charged fees for applying for credentials. I propose that there be no fees for individuals at this stage. This will ensure that there is no financial barrier to individuals using the Service, in order to promote uptake.

**Crown funding**

23 The Department was appropriated funding in the 2011 Budget for 2011/12 and 2012/13 for the govt services, and Cabinet noted that ongoing funding will be required [EGI Min (11) 4/11]. I will be seeking decisions through the Budget process on funding for 2013/14 and subsequent years. This Crown funding will reduce quickly as the Service recovers its costs through charges.

**Duration of credentials**

24 An electronic identity credential is the electronic record that supports an individual’s ability to use the Service. Regulations are required to set the duration period for the life of a credential which may be renewed upon application for further periods. I propose that this period be set at five years. This will enable robust checks to be undertaken periodically to detect fraudsters who may have obtained a credential fraudulently previously, and to ensure
individuals are not wrongfully using someone else's electronic identity credential. The period aligns with the current duration of a New Zealand passport and therefore would enable New Zealanders to apply for a passport and a credential at the same time.

25 I also propose that, when people apply to renew their credential before it expires, the duration for their new credential should run from the date of the expiry of their current credential provided that there is no more than three months' extra validity. This will encourage people to keep their credentials active, while also ensuring that the information for the credentials is up to date.

26 While the Bill allows for different periods to be set for children under 14 years of age, I do not propose to set a different period at this stage.

Retention of information

27 The Bill provides for regulations to prescribe how long the Department can retain an individual’s personal information following the cancellation, expiry or revocation of a credential. This regulation-making power was recommended by the Government Administration Committee to ensure there are transparent controls for the retention of information by the Department.

28 I propose the following time periods be set:

<table>
<thead>
<tr>
<th>Circumstances</th>
<th>Retention period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential cancelled on application by individual</td>
<td>11 years</td>
</tr>
<tr>
<td>Expired credential</td>
<td></td>
</tr>
<tr>
<td>Credential cancelled due to death of person</td>
<td></td>
</tr>
<tr>
<td>Credential relating to the original identity of a person in the witness</td>
<td></td>
</tr>
<tr>
<td>protection programme that has been cancelled as a new credential has been</td>
<td></td>
</tr>
<tr>
<td>issued in the new identity</td>
<td></td>
</tr>
<tr>
<td>Credential that was issued to an undercover Police or New Zealand Security</td>
<td>1 month</td>
</tr>
<tr>
<td>Intelligence Service (NZSIS) employee and is no longer needed</td>
<td></td>
</tr>
<tr>
<td>Credential revoked by either the Chief Executive or a court (on the basis</td>
<td>Not specified in</td>
</tr>
<tr>
<td>of false or fraudulent representation, or error)</td>
<td>regulations</td>
</tr>
</tbody>
</table>

29 These timeframes provide sufficient time for the Department to identify fraud, whilst also protecting the rights of individuals. An 11-year timeframe (just over twice the proposed duration of credentials) for most situations provides sufficient time for the Department to update its facial recognition software to detect previous fraud. The Department will have two opportunities for fraudulently-issued credentials to be detected during renewal processes.

30 Credentials issued to undercover Police and NZSIS employees that are no longer necessary should be deleted quickly – a one-month retention period would be an appropriate maximum retention period. This period would apply from when the Police or NZSIS advise the Department that the credential and associated information is no longer needed for their purposes.
31 I propose not to regulate a retention period for information when credentials have been revoked. Credentials may be revoked either on the basis of error, or false or fraudulent representation. By not regulating, decisions about the retention of information will be made in line with information privacy principle 9 in the Privacy Act 1993. This provides that information shall not be kept for longer than is required for a lawful purpose. This means that, for example, information about credentials revoked on the basis of false or fraudulent representation could be retained for the life of the individual to whom the credential relates. However, when a credential is revoked on the basis of error a decision could be made to delete that information more quickly.

32 The Bill provides that different periods could also be set for different types of information regulated by the Bill – such as photographs (collected for processing applications), the records of usage history (a history of when an individual has used the Service with participating agencies, but not including details of the transactions) and the information in electronic identity credentials. However, I do not believe there is any advantage in retaining some information for different periods as all the information would be relevant for investigating fraud and protecting individuals' rights.

**Identity information checks**

33 The Bill allows for regulations to declare agencies that may provide identity information checks. These checks allow the Department to confirm whether the information presented by an applicant is consistent with the information that another agency holds. This process will be used when the Department is not confident about a person’s identity and cannot use information matching programmes (for instance, where the person does not have a passport). I propose that checks may occur with the following agencies:

1. Hospitality New Zealand (18+ Cards);
2. the New Zealand Police (firearm licences); and
3. the New Zealand Transport Agency (driver licences).

**Commencement date**

34 Most of the provisions of the Bill need to be brought into force by an Order in Council to ensure the necessary computer system and support processes are completed before the legislation comes into effect. Subject to the Bill's passage through the House, I propose a commencement date of 1 March 2013.

**Consequential amendment to anti-money laundering code of practice**

35 In 2011 the then Ministers of Finance, Commerce and Internal Affairs issued the Identity Verification Code of Practice (the Code) under the AML/CFT Act. The Code provides a 'safe harbour' for reporting entities (banks, casinos and other financial institutions) to follow when verifying the identity of their customers. If Cabinet agrees to allow reporting entities to use the Service, the Service will be an effective tool for those agencies to meet their obligations under the AML/CFT Act.
36 Concerns have been raised that the current wording in the Code requires a standard of identification that is not consistent with that provided by the Service or any other electronic identity verification providers. There are also other minor technical changes which could be made to ensure the Code operates as intended. Typically, any changes to the Code would need to be made through a public consultation and Cabinet process. However, given the minor and technical nature of the changes needed, I propose that Cabinet authorise the Ministers of Finance, Commerce and Internal Affairs, in consultation with the Minister of Justice, to undertake the required consultation process and make the necessary changes.

Consultation

37 The following agencies were consulted in the development of this paper: the Financial Markets Authority, the Ministry of Business, Innovation and Employment, the Ministry of Justice, the Ministry of Social Development, the New Zealand Police, the New Zealand Security Intelligence Service, the New Zealand Transport Agency, the Office of the Privacy Commissioner, the Reserve Bank of New Zealand, the State Services Commission, and the Treasury. New Zealand Post Limited was also consulted because of its partnering role to support the igovt services’ operations. The Department of the Prime Minister and Cabinet and the Parliamentary Counsel Office were informed.

38 The Bill requires that the Minister of Internal Affairs must consult with the Privacy Commissioner on the regulations prescribing the period for which information may be retained. The Office of the Privacy Commissioner has been consulted on this paper and supports the proposals. The Office of the Privacy Commissioner will also be consulted during the drafting of the regulations.

Financial implications

39 The proposals in the paper do not have any direct financial implications. Charges for agencies using the Service will subsequently be set by agreements with the Chief Executive of the Department or New Zealand Post.

Human rights implications

40 The proposals in this paper appear to be consistent with the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993. A final view as to whether the proposals will be consistent with the New Zealand Bill of Rights Act will be possible once the regulations have been drafted.

Legislative implications

41 This paper seeks approval to issue drafting instructions to the Parliamentary Counsel Office to prepare regulations. I intend to bring these regulations to the Cabinet Legislation Committee once the Bill is enacted.

Regulatory Impact Analysis

42 The Regulatory Impact Analysis requirements apply to these proposals. A Regulatory Impact Statement (RIS) is attached to this paper.
The Chair of the Department’s Regulatory Impact Analysis Panel has reviewed
the RIS and associated supporting material and considers that the information
and analysis summarised in the RIS meets the quality assurance criteria.

I have considered the analysis and advice of my officials, as summarised in the
attached RIS, and I am satisfied that the regulatory proposals recommended in
this paper:

- are required in the public interest;
- will deliver the highest net benefits of the practical options available;
  and
- are consistent with our commitments in the Government statement
  “Better Regulation, Less Regulation.”

Publicity

Subject to Cabinet’s agreement to the proposals and following enactment of the
Bill, I will make announcements about the intention to promulgate regulations to
support the implementation of the Bill. I intend to make announcements about
the decisions on participating agencies, including the policy framework, and on
the agreement for joint Ministers to undertake the required consultation process
and make necessary changes to the AML/CFT Identity Verification Code of
Practice. This is to provide assurance to the market on these issues ahead of
regulations being promulgated. I also intend to proactively release this paper,
subject to consideration of any deletions that would be justified if the information
had been requested under the Official Information Act 1982 (CO Notice (09) 5).

Recommendations

The Minister of Internal Affairs recommends that the Cabinet Economic Growth
and Infrastructure Committee:

1. note that the Electronic Identity Verification Bill (the Bill), which governs the
   identity verification service (the Service) enabling individuals to prove their
   identity online, was reported back by the Government Administration
   Committee on 19 June 2012, had its second reading on 29 August 2012
   and has a Priority 2 on the 2012 legislative programme;

Participating agencies

2. note that the Bill requires regulations to declare agencies as participating
   agencies to use the Service;

3. agree that all public sector agencies (including local government and
council-controlled organisations) and registered banks be listed as classes
of participating agencies;

4. agree that the policy framework based on necessity, trust, alternative
   service accessibility and usability (as expanded in Appendix A) be used for
determining whether private sector agencies should be declared as
participating agencies to use the Service;
Fees and charges

5. note that the Service’s success will rely on the Service achieving full cost recovery over time;

6. note that the Bill enables fees and charges to be set either by regulation or by agreements with participating agencies, and allows for fees to be set for individuals;

7. agree that, at this stage, charges for participating agencies be set by agreements and not by regulations and that there be no fees prescribed for individuals, as regulated fees may discourage uptake during the start-up phase of the Service;

Duration of credentials

8. note that the Bill requires regulations to specify the length of time for which an electronic identity credential (the electronic record an individual uses to prove his or her identity) is valid;

9. agree that electronic identity credentials be valid for five years, with renewed credentials valid from the expiry of the previous credential for up to three months’ additional validity;

Retention of information

10. note that the Bill allows regulations to specify the period for which the Department of Internal Affairs may retain information after an electronic identity credential is cancelled, is revoked or expires;

11. agree that information relating to:
   a) a credential cancelled on application by the individual to whom it relates be retained for 11 years;
   b) expired credentials be retained for 11 years;
   c) a credential cancelled due to the death of the individual to whom it relates be retained for 11 years;
   d) a credential relating to the original identity of a person in the witness protection programme that is cancelled when a new credential is issued in the person’s new identity be retained for 11 years;
   e) a credential that was issued to an undercover Police or New Zealand Security Intelligence Service employee and is no longer needed be retained for 1 month;
   f) a credential revoked by either the Chief Executive of the Department of Internal Affairs or a court (on the basis of false or fraudulent representation, or error) not be subject to a regulated retention period;

12. note that the Bill requires the Minister of Internal Affairs to consult with the Privacy Commissioner before recommending to the Governor-General to the making of this regulation, and that the Office of the Privacy Commissioner has been consulted on this paper and will be consulted during the drafting of the regulations;
Identity information checks

13. **note** that the Bill will enable the Department of Internal Affairs to check whether an individual’s identity information is consistent with information held by agencies specified in regulations;

14. **agree** that Hospitality New Zealand (18+ Card), the New Zealand Police (firearm licence) and the New Zealand Transport Agency (driver licence) be declared as agencies with which such identity information checks can take place;

Commencement date

15. **agree in principle**, subject to the Bill’s passage through the House, that the Bill’s commencement date be 1 March 2013 and that this be confirmed by the Cabinet Legislation Committee;

Drafting instructions

16. **invite** the Minister of Internal Affairs to issue drafting instructions to give effect to the above decisions;

Consequential amendment to the Identity Verification Code of Practice

17. **authorise** the Ministers of Finance, Commerce and Internal Affairs, in consultation with the Minister of Justice, to issue a public consultation document and make necessary changes to the Identity Verification Code of Practice 2011 (issued under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009) to reflect the Service being made available to private sector agencies and to make other minor technical amendments to ensure the Code of Practice operates as intended; and

Publicity

18. **agree** that the Minister of Internal Affairs:

a) announce the decisions on participating agencies, including the policy framework, and on the agreement for Ministers to undertake the required consultation process and make necessary changes to the Identity Verification Code of Practice; and

b) pro-actively release this Cabinet paper, subject to consideration of any deletions that would be justified if the information had been requested under the Official Information Act 1982.

Hon Chris Tremain  
Minister of Internal Affairs

7/11/2012
Appendix A: Proposed policy framework for participating agencies

Necessity
- The agency must have a legitimate need to use the identity verification service due to the nature of the agency’s undertaking or activity.
  - This need should either be established by law or based on analysis of the nature of the risks faced by the agency.

Trust
- The agency must have appropriate and effective measures in place for ensuring compliance with the Electronic Identity Verification Act 2012, the Privacy Act 1993 and other relevant legislation. Factors that may be taken into account include:
  - Whether the agency has been found in breach of the Electronic Identity Verification Act, the Privacy Act or other relevant legislation within the past five years; and
  - If an agency has previously been found in breach of the Electronic Identity Verification Act, the Privacy Act or other relevant legislation, whether the agency has put in place appropriate policies and practices to adequately address those issues.
- The agency must be stable - it must be an organisation that is established by law or can otherwise demonstrate it has an established basis.

Alternative service accessibility
- The agency must provide alternative means for customers to verify their identities (when required to do so), so far as is practicable for the agency in the circumstances.

Usability
- The agency must be able to use the identity verification service (such as having the correct technical infrastructure).
- The agency must be able to meet any standards or specifications set by the Chief Executive of the Department of Internal Affairs under the Electronic Identity Verification Act.
- The agency’s customers must be likely to be able to use the identity verification service (for instance, it may not be appropriate for the Service to be used by overseas-based individuals for one-off transactions).
- The identity verification service must be legally sufficient for the agency’s requirements for electronic identity verification.
- If the identity verification service does not meet all of the agency’s requirements (e.g. the agency is required by law to collect information that the identity verification service does not provide), then there must be readily available means of meeting those requirements, whether through a product offered in conjunction with the identity verification service or some other process.