INFORMATION
INTEGRITY
SOLUTIONS

NATIONAL TRUSTED IDENTITIES FRAMEWORK (NTIF)

DISCUSSION PAPER

For: Department of Prime Minister and Cabinet

26 SEPTEMBER 2012

TABLE OF CONTENTS

1 INTRODUCTION

Information Integrity Solutions (IIS)[1] has been engaged to assist the Department of Prime Minister and Cabinet (PM&C) to conduct consultations with key stakeholders, across the government, business and community sectors, on the steps necessary to improve trust in the digital environment. A key part of this is to develop a National Trusted Identities Framework (NTIF). This document is designed to facilitate this consultation. The details of the consultation process are set out in Section 6.

2 THE CHALLENGE — STIMULATING GREATER TRUST ONLINE

To do business or provide services effectively online, organisations (including governments) need to be sure that the person they are dealing with is trustworthy. At the same time, for people to fully participate in the online economy, they need to trust organisations and service providers. Both need to feel comfortable with and understand security and privacy arrangements.

For some, this is not currently the case resulting in less than full participation in the digital economy. The media regularly reports on online scams, significant data breaches and identity fraud as we grapple with how to safely and securely ‘digitise’ identities.

Organisations and government agencies build their own solutions for delivering trust, each with its own user name and password or other mechanisms for administering it. Each solution has its own checks to verify identity and many ask for more identity information than they need about a person. While these solutions meet the separate needs, they are not designed to be interoperable and cannot easily share resources.

In turn, people must use each solution separately and often in very different ways. People need to manage an array of credentials, including usernames, passwords and cards. They have little or no control over what identity and other personal information they are asked to provide for accessing services. Once the information is given, they have little visibility over what it is being used for, who accesses it, or where to go when there is a problem. For many people this is annoying or unsettling but for some this is just too high a price to pay for online services.

At the same time, private sector activities to stimulate trust appear to have been slowed by perceptions this is not an area in which profit can be made. For this and a number of other reasons a national market for the provision of convenient and interoperable digital identity services has not developed in Australia. Similar to the US, UK, Canada and NZ, Australia recognises the importance of supporting the development of this fledgling market to meet the identity management needs of society and governments as they continue to adopt online services for more personal and more sensitive interactions.

The ability to improve overall trust in the online environment will greatly assist in reducing the current inefficiencies for business and government and lack of data protection and convenience for people. Key jurisdictions, such as the US, UK, Canada and NZ have recognised that a key part of the solution is to develop an overarching framework for establishing trust among participants in the area of digital identities that would cover both public and private sector. In Australia’s case we are calling

[1] Information about IIS can be found at www.iispartners.com.

this a National Trusted Identities Framework (NTIF). While increasing trust, such a framework could also create an environment of greater certainty in which the private sector may feel more confident about developing and providing relevant services.

Building trust online and creating a market — the long-term vision. An NTIF could promote the development of a national market in digital identity products and services. By applying consistent standards for all participants in this market, an NTIF could allow a digital identity that is trusted by one participant (such as a bank) to be trusted by another (such as a government agency). Enhanced online trust and security will bring new opportunities and a greater willingness to develop innovative ideas to drive Australia's economy. This would lead to improved access to services, new products and markets for consumers and industry, and more productive ways of doing business.

An NTIF would be citizen-centric, voluntary and would seek to enhance the privacy of individuals and businesses by giving people control over the disclosure of their personal information. An NTIF would be a collaborative venture aimed at achieving trust in the digital identities of individuals, businesses, government agencies, other organisations and devices. In this way, an NTIF would be one of the enablers of the future digital economy by helping users take full advantage of the social benefits and commercial opportunities available through greater online engagement.

While this consultation has an eye to the long-term vision, its aim is to understand how to reach a medium-term point. Then, developments in the digital identity space can be examined, and the progress of larger partner economies reassessed.

3 CONSEQUENCES OF FAILURE TO ACT

Without a national framework that provides a coordinated response to the issue of trusted identities and which supports the developing digital identity services market to provide the required trusted services and products there is a risk:

- For business that:
    - it will not get the assistance in managing identity information that it needs;
    - it will not gain the efficiencies that can be derived from mutual trust and reliance on others' credentials or verified identity information;
    - it is shut out of opportunities to provide digital identity services that it is well positioned to provide; and
    - government will impose identity information requirements that are expensive and difficult to meet.
- For people that:
    - they do not trust initiatives being developed because the agenda for having them is not clear (for example, is it to address government risks? private sector risks? or a person's risks?);

  - unexpected big picture privacy, security, usability or access issues arise because there is no coordinated overview of all the initiatives being undertaken or the way all the initiatives fit together;
  - solutions do not give people the control and choices that they want and need in order to create trust and confidence in the online environment; and
  - they may not take full advantage of the social benefits of the online environment.
- For government that:
  - it may continue to undertake digital identity services that could be more efficiently and effectively delivered by the private sector;
  - it may not develop policies that best support the digital economy and Australia's diverse needs;
  - it may impose undue or too light regulation on providers of digital identity services and products resulting in stifling the market or a lack of protection for privacy and personal data;
  - options are implemented that will lock the government into solutions that become rapidly out-of-date or hard to change or expensive to change in the future;
  - it develops initiatives that are not scalable or viable because they are not relevant to the risks that other agencies or private sector organisations face;
  - its initiatives will unnecessarily duplicate or overlap efforts being undertaken elsewhere in government or the private sector (or vice versa); and
  - its solutions developed are not interoperable, or easily interoperable with other government, private sector or international initiatives or approaches.
- For Australia :
  - digital productivity within Australia will not be fully realised. Many Australians may not fully seize the potential opportunity to increase productivity and enable innovation. Some Australians may not engage in online activities due to a lack of trust;
  - international competiveness will decline as other nations adopt strategies to maximise the productivity of their digital economies. Many countries are already more advanced than Australia; and
  - international online transactions will be hampered by a lack of interoperability.

4 STEPS SO FAR

The government began this process of considering what might be needed to achieve trust in the online environment with the *Cyber White Paper Public Discussion Paper* (2011) and the *Cyber White*

Paper Policy Proposal: National Trusted Identities Framework (2011). Recognising the critical importance of involving all key sectors of Australia in the process, it also began consultations with all key public, private sector and community stakeholders at a workshop held at National ICT Australia in Sydney in 20 December 2011. These were the first steps in considering whether a national trusted identities framework might be needed.

The key conclusions from this consultation were:

- that the scope of an NTIF needed to be more clearly defined in order to determine such matters as:
    - the level of government involvement needed to create a viable market
    - the standards and accountability needed
    - the kind of technologies that might need to be developed or deployed;
- business and individuals must be able to see "what's in it for them" in order for there to be a viable market; and
- that a mix of government and private sector involvement in an NTIF is appropriate with government having a leadership role but with private sector providing services where efficient, viable and appropriate taking into account usability, privacy, security and equity of access.

Noting the risks of inaction, the Government is committed to the development of a NATIONAL trusted identities framework (NTIF). Building on the valuable engagement with key stakeholders that began in December 2011, the Government has been refining the scope of the NTIF and the options available for progressing it. The following sections aim to do this.

5 AREAS OF FOCUS FOR AN NTIF ROADMAP

5.1 KEY ACTIVITIES

The NTIF vision requires attention to the following areas in order to promote trust in digital identities and the online environment generally in a cost effective and efficient way:

1. The creation of a national market for trusted digital identity services.
2. The adoption of an overarching framework that provides national governance for digital identities.
3. The adoption of consistent identity rules and standards that allow trust arrangements between disparate online systems (e.g. inter-federation).
4. The enhancement of people's control over their privacy and personal data online.

5.2 REALISTIC TIMEFRAME

The NTIF goal of an efficient market providing trusted digital identity services is not achievable in the short-term due to key gaps. These include viable economic models, governance arrangements, national rules and standards and lack of user-centric tools that empower people and enhance privacy while ensuring security.

Therefore, developing a roadmap for how to begin to fill the gaps– say within the next 3-5 years – would seem to be the most practical approach. Attempting to plan activities beyond this is unlikely to be useful in such a dynamic environment where solutions are rapidly evolving.

A mid-term approach will also enable Australia to be informed by international developments. Australia's strategic partners are more advanced in their journey to the shared vision, and are also each taking a slightly different approach with their roadmaps. This approach will enable Australia to benefit from their experience in deciding its longer term strategy.

5.3 Focus on government role first

In developing a national market for trusted digital identity services, it seems practical for the roadmap to first focus on the Government's role in encouraging this market. It is in the best position to undertake a number of key first steps that are achievable in within the next 2-3 years. These include:

- **Enable market**: It is in the best position to undertake foundational market enabling activities such as establishing and implementing overarching governance structures that provide for close and sustained multi-stakeholder involvement, including the development and implementation of consistent rules and standards and possibly some pilot activities
- **Extend government services:** It can expand its existing reform initiatives to see how they may be able to address known issues in a way that could benefit the whole economy, or lead by example
- **Raise awareness:** It is well positioned to undertake national awareness raising activity about the need for safe and secure use of digital identities and the need for people to exercise as much control as possible over their digital identity information.

Building on these activities the Government is also in a very strong position to influence the market in digital identity services. It has very significant demand for high-integrity digital identity services and is in a position to influence the market depending on the extent to which it continues to keep meeting this demand itself, or whether it moves to an approach where it looks to the private sector to take over the supply of these services or to provide new services to meet this demand.

Should the private sector become a key supplier to government, the government is also in the position to drive further demand for digital identity services by mandating their use across government. This could trigger further private sector activity in the market. For example, private suppliers could offer the 'ex-government sector' services to other sectors e.g. financial institutions, or develop value-add products on the back of the core solutions suite.

6 APPROACH TO A ROADMAP

Taking into account the focuses proposed above, the following steps and options for an NTIF roadmap are outlined for consideration and consultation.

6.1 Steps for 2013-2014

During this period the key activities would be to take steps that are achievable and would lay the foundation for further market development.

The most important of these would be market enabling activities to establish a trust framework and following from that standards and rules which would enable a digital identity market by creating certainty, interoperability and the necessary privacy and security protections.

At its most basic level, these are likely to consist of:

- identifying the key roles of participants in providing digital identity services;
- developing standards and policies that each participant must meet or comply with in order to be trusted and able to interoperate with participants in other trust frameworks, for example:
    - data quality
    - protecting privacy
    - protecting security
    - technical interoperability
    - customer service and complaints handling
    - process for approval/accreditation; and
- an overarching structure to make sure governance is coordinated and trust is built in a way that meets government, private sector and community needs and requirements.

Other key activities would be those that extend government services and raise awareness as identified above.

6.2 Options for further steps – 2015-2016

In the following period three possible options for government activity in progressing NTIF activity are proposed for discussion.

6.2.1 Enable option

In this option, having undertaken the foundational activities outlined for the period 2013-2014, before undertaking any further activity, the government would assess the impact of these activities on the development of a market that provides safe, secure and trusted digital identity services. It would also consider developments internationally to assess whether there are developments there that could be used in Australia. Taking into account these outcomes and developments, new priorities and steps for meeting the NTIF vision would be developed.

6.2.2 Encourage option

In this option, the government, without assessment of the foundational activities, would take two additional steps to influence the development of a market in trusted digital identity services. These would be:

- to require all government agencies to try to have their digital identity needs met by the private sector and only if this is not achievable would agencies be able to develop the solutions themselves; and
- at the same time, the government would take measured steps to transition the services it currently provides into the hands of the private sector.

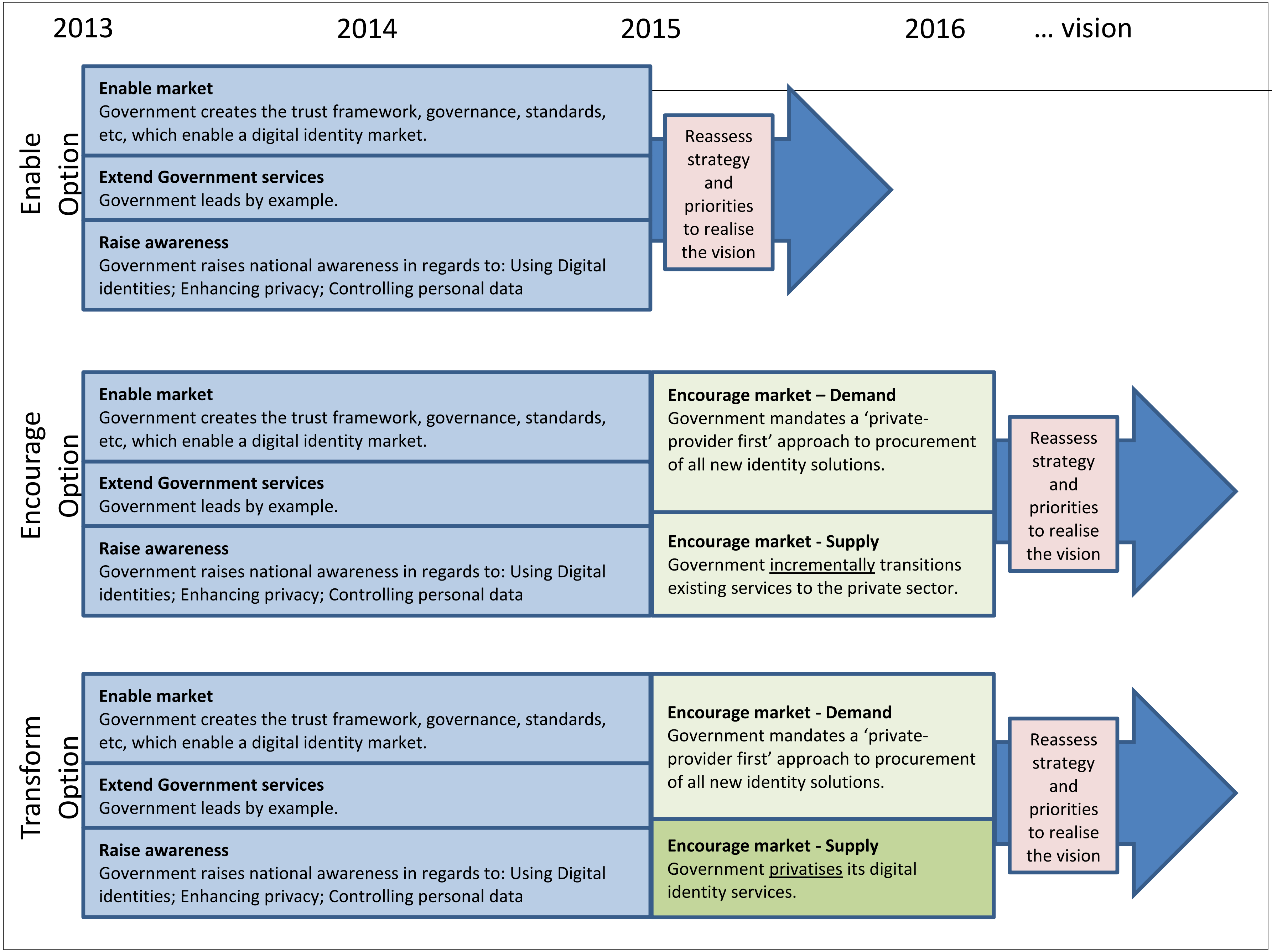
Following this, the government would reassess the success of these steps in stimulating a market.

6.2.3 Transform option

In this option, without assessment of the foundational activities, the government would:

- require all government agencies to try to have their digital identity needs met by the private sector, and only if this is not achievable, would agencies be able to develop the solutions themselves; and
- in one move, privatise all of its digital identity services.

A diagram setting out each of the options is below.



2013 2014 2015 2016 … vision

Enable Option

Enable market
Government creates the trust framework, governance, standards, etc, which enable a digital identity market.

Extend Government services
Government leads by example.

Raise awareness
Government raises national awareness in regards to: Using Digital identities; Enhancing privacy; Controlling personal data

Reassess strategy and priorities to realise the vision

Encourage Option

Enable market
Government creates the trust framework, governance, standards, etc, which enable a digital identity market.

Extend Government services
Government leads by example.

Raise awareness
Government raises national awareness in regards to: Using Digital identities; Enhancing privacy; Controlling personal data

Encourage market – Demand
Government mandates a ‘private-provider first’ approach to procurement of all new identity solutions.

Encourage market - Supply
Government incrementally transitions existing services to the private sector.

Reassess strategy and priorities to realise the vision

Transform Option

Enable market
Government creates the trust framework, governance, standards, etc, which enable a digital identity market.

Extend Government services
Government leads by example.

Raise awareness
Government raises national awareness in regards to: Using Digital identities; Enhancing privacy; Controlling personal data

Encourage market - Demand
Government mandates a ‘private-provider first’ approach to procurement of all new identity solutions.

Encourage market - Supply
Government privatises its digital identity services.

Reassess strategy and priorities to realise the vision

8 CONSULTATION PROCESS

8.1 THIS PAPER

The issue of addressing trust in the online environment is potentially very broad and hard to grapple with in a meaningful and practical way. As a result, this paper seeks to set out the issues in a way that:

- reflects the current government policy and programme environment;
- seeks to narrow down the proposed focus of activity to the extent possible; and
- gives as much detail as possible on possible approaches and takes into account what is realistic to achieve in the medium term (3-5 years).

In this way it hopes to facilitate detailed, practical and constructive comment that will be useful input to the business case that PM&C is preparing.

The will be distributed to stakeholders and will form the basis for consultations.

8.2 CONSULTATION METHODS

PM&C has commissioned Information Integrity Solutions to conduct consultations which include:

- two combined stakeholder workshops on 10 October and 30 October (invitees will be those who were involved in the 20 December 2011 group with some possible additional stakeholders to fill any sectoral gaps);
- meetings or workshops with particular sectors;
- some face to face meetings if particularly asked for or desirable; and
- the chance to provide written feedback on the Discussion Paper.

8.3 QUESTIONS FOR CONSULTATION

Do you understand how a digital identity services market could assist with increasing online trust?

Do you have a mental “picture” of a national market for trusted identity services? What are its key features? Who are the main actors?

Do you think the benefits of a national framework justify investment in it? What are the consequences of not having an NTIF?

Do you think there is a role for federal government in order to achieve a viable national market for safe and useable identity services?

If so, what do you think is the best way for government to get involved?

- facilitating the development of a national governance framework?
- stimulating either supply of or demand for digital identity services or both?

Which particular strategies for stimulating supply or demand do you think the government should focus on first? Should they do one or both?

What identity services do you think government should continue to provide for the next 5 years versus long-term? For example,

- should it continue as the authoritative source of identity data through birth certificates, passports, drivers' licences?
- should it continue to provide its own digital identity services such as social services cards, digital certificates for businesses, user accounts and passwords?
- should it continue to provide validation services for key identity documents, digital credentials and digital signatures?

Which of the three options for creating a market outlined in the paper do you think the government should adopt?

What would the government need to do, at a minimum, to encourage private players to offer digital identity services?

- Is it simply a matter of there not being clear standards around? If so, what particular standards are needed? For example, are standards needed for technical design, technologies, business design to ensure interoperability, privacy, useability, and individual control.
- Or is it because there are no current private sector drivers (and thus government would need to go to market to stimulate change)?

8.4 METHODS OF PROVIDING FEEDBACK

IIS will handle feedback from you on this paper and is responsible for organising and holding meetings.

You can provide feedback in the following ways:

- **Email** feedback to: Christine Cowper at ccowper@iispartners.com
- Call: Fixed line – 02 8303 2438 or mobile – 0402 847 925
- Ask for a meeting:

We would like to receive feedback by COB **Wednesday 24 October** 2012.