

# Introducing integrated e-government in Australia

Arvo Ott, Fergus Hanson and Jelizaveta Krenjova

Policy Brief  
Report No. 11/2018



## About the authors

**Dr Arvo Ott** joined the e-Governance Academy, a non-profit think tank and consultancy organisation in Estonia, on 1 November 2005. His main responsibilities include the coordination of e-governance studies (e-government and e-democracy aspects), training programs and general management. Prior to joining the e-Governance Academy, Dr Ott served as the head of Department of State information systems (head of e-government office) at the Ministry of Economic Affairs and Communications for 12 years. He was responsible for Estonian information society and e-government strategy planning, and legal, organisational and technical architecture development and implementation. During the last several years, Dr Ott took part in many international projects and programs on e-governance (including information society policy and e-participation advice, e-government interoperability aspects, organisation development and planning).

**Fergus Hanson** is the head of ASPI's International Cyber Policy Centre. He is the author of *Internet wars* and has published widely in Australian and international media on a range of cyber and foreign policy topics. He was a visiting fellow at the Brookings Institution and a Professional Fulbright Scholar based at Georgetown University working on the take-up of new technologies by the US Government. He has worked for the United Nations and as a program director at the Lowy Institute and served as a diplomat at the Australian Embassy in The Hague. He has been a fellow at Cambridge University's Lauterpacht Research Centre for International Law and the Centre for Strategic and International Studies, Pacific Forum.

**Jelizaveta Krenjova** is a project manager at the e-Governance Academy in Estonia. Previously, she managed a long-term local government project in Ukraine that focused on strategic support to e-governance development and on the implementation of technical e-government solutions in four cities and one regional state administration in the western part of the country. Apart from e-government projects, Jelizaveta is involved in the work of the e-democracy domain of the e-Governance Academy, providing advice and conducting research in the field of e-participation instruments. Jelizaveta earned her PhD from the Ragnar Nurkse Department of Innovation and Governance at Tallinn University of Technology. Her research interests comprise participatory instruments at the local level.

## What is ASPI?

The Australian Strategic Policy Institute (ASPI) was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

## ASPI International Cyber Policy Centre

The ASPI International Cyber Policy Centre's mission is to shape debate, policy and understanding on cyber issues, informed by original research and close consultation with government, business and civil society.

It seeks to improve debate, policy and understanding on cyber issues by:

1. conducting applied, original empirical research
2. linking government, business and civil society
3. leading debates and influencing policy in Australia and the Asia-Pacific.

We thank all of those who contribute to the ICPC with their time, intellect and passion for the subject matter. The work of the ICPC would be impossible without the financial support of our various sponsors, but special mention in this case goes to the Australian Computer Society (ACS), the New South Wales Government and the Victorian Government, which have supported this research.

## Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

## ASPI

Tel +61 2 6270 5100

Fax + 61 2 6273 9566

Email [enquiries@aspi.org.au](mailto:enquiries@aspi.org.au)

[www.aspi.org.au](http://www.aspi.org.au)

[www.aspistrategist.org.au](http://www.aspistrategist.org.au)

[facebook.com/ASPI.org](https://www.facebook.com/ASPI.org)

[@ASPI\\_ICPC](https://twitter.com/ASPI_ICPC)

[www.aspi.org.au/icpc/home](http://www.aspi.org.au/icpc/home)

© The Australian Strategic Policy Institute Limited 2018

This publication is subject to copyright. Except as permitted under the *Copyright Act 1968*, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers.

First published October 2018. Cover image: Abstract technology background. © [sadsadang/iStockphoto](#).



# Introducing integrated e-government in Australia

Arvo Ott, Fergus Hanson and Jelizaveta Krenjova

# Contents

<b>Foreword</b>	<b>03</b>
<b>What's the problem?</b>	<b>04</b>
<b>What's the solution?</b>	<b>04</b>
<b>Introduction</b>	<b>05</b>
<b>E-government in Australia</b>	<b>05</b>
<b>An integrated approach to e-government in Australia</b>	<b>07</b>
The once-only principle	07
A decentralised approach	07
A digital identity	08
Privacy	08
A joined-up back office	09
Evaluating outcomes from government-funded services	09
Other issues	09
Lessons learned from abroad	10
<b>Recommendations</b>	<b>11</b>
<b>Notes</b>	<b>12</b>
<b>Acronyms and abbreviations</b>	<b>13</b>

## Foreword



With the 2016 distributed denial of service attack on Australia's first fully digital Census and Centrelink's 2017 automated debt-recovery system glitches still fresh in our minds, it would be easy to pause in the pursuit of digitising government services.

The reality, however, is that there are compelling benefits to expediting government digital transformation, and the case for change is not simply one of customer convenience.

Deloitte Access Economics has estimated that the federal and state governments conduct 811 million citizen transactions each year. It calculated that lifting the share of transactions performed digitally from 60% to 80% over a 10-year period would lead to government productivity benefits worth \$17.9 billion, plus a further \$8.7 billion in benefits to citizens.

But the benefits of integrated digital government services extend even beyond time and resources saved. Data is the fuel for many new business models and, according to OECD measures, right now Australia performs only moderately well compared to international peers, particularly in relation to the availability of open government data.

The OECD has estimated that adopting more data driven decision-making in government has potential output and productivity benefits of 5% to 6% in the US, while improving data quality and access by 10% could increase labour productivity by an average of 14%.

That can have additional flow-on effects across the economy. Almost 2 million people are employed in the three levels of government in Australia, meaning that 16% of the country's 12.5-million-strong workforce is employed in the public sector. This represents a strategic capability, enabling knowledge and skills transfer across the broader economy.

Based on previous productivity gains from technology take-up, that can have significant benefits for Australia's output. Further adoption of digital technologies across the economy has the potential to add an extra \$66 billion to Australia's GDP over the next five years alone.

So the case for change is clear; the question is really about how to do it. How do we maximise the opportunities, while best protecting citizens' data and privacy? This policy brief is intended to start that conversation.

Yohan Ramasundara

President, Australian Computer Society

## What's the problem?

Australia was an early leader in the digitalisation of government services, and some Australian Government departments and state governments have continued to innovate and deliver enhanced services online. However, in the global context, Australia has now fallen behind and has so far failed to adopt an integrated approach to e-government that joins up all government services across all three tiers of government. For citizens, this makes life harder than it needs to be and consumes time that could be spent on other things. For businesses, it increases transaction costs. Although existing user interfaces are logical and user-friendly, there's still a limited amount of third-stage e-services enabling two-way interactions between citizens and governmental institutions.<sup>1</sup> Critical missing pieces inhibiting the flourishing of e-services are a properly functioning digital identity ecosystem and a digital signature.<sup>2</sup>

## What's the solution?

The Australian Government should launch a consultation with the states and local governments to develop an integrated approach to e-government that joins up all services from all three tiers of government. The model will need to be customised to Australia's unique circumstances but should be designed to reduce business transaction costs, allow citizens to engage seamlessly with the federal, state and local governments and prioritise citizens' control and ownership of their data.

A decentralised architecture should be used to ensure there's no single point of failure and to allow easy and secure integration with existing digital government platforms. The federal government should provide essential enabling systems:

- a digital identity (eID)—one has already been developed by Australia Post, and a second is being built, but significant work is needed to allow eID to take root
- the legal, organisational and technical preconditions for a digital signature—legislation should ensure that the digital signature has equal legal weight to a traditional handwritten signature
- secure data exchanges between different government IT systems.

## Introduction

Integrated Australian e-government would mean that less of citizens' and businesses' time would be wasted engaging with government. A digital signature would make official transactions simple: signing contracts or submitting applications could be done in moments. Mindless hassles when moving between jurisdictions (such as swapping licences from one state to another) would evaporate overnight; there would be no need to conduct 100-point identity checks in person, and time-consuming visits to physical government offices would become a thing of the past. In Estonia, where e-government is a national passion, officials estimate that these efficiencies lift annual GDP by 2%.<sup>3</sup>

While many government departments already have user-friendly online portals, and some states have begun integrating several services within single online platforms (such as Service NSW and Service Victoria<sup>4</sup>), Australia has yet to attempt a citizen-centric approach that makes citizen and business engagement with all three tiers of government seamless. It also lacks critical enabling systems. The major building blocks needed to achieve an integrated approach to e-government are an integrated government back office and a simple, easy-to-use and secure eID and digital signature.

That isn't to downplay the practical challenges of joining up three tiers of government that have historically resisted cooperation or the attention to detail needed to address cybersecurity challenges. Joined-up e-government is nonetheless essential to a high-functioning 21st-century economy and should be attempted.

## E-government in Australia

Australia was initially quick to join the global e-government trend, and even developed an international reputation as an early leader in this area (peaking around 1999).<sup>5</sup> However, a joined-up approach to e-government wasn't achieved.<sup>6</sup> The success of some large departments, such as the Australian Taxation Office and Centrelink, has depended more on a joined-up 'front end' rather than an integrated back end that allows citizens to engage with government seamlessly.<sup>7</sup>

A national identification scheme (the Australia Card) was proposed in the 1980s. However, the Australia Card Bill generated significant public concerns about privacy and was defeated in the Senate.<sup>8</sup> In 2006, Prime Minister John Howard made another attempt with the Access Card,<sup>9</sup> before it too was shut down by the Rudd government in 2007.

The *Electronic Transactions Act 1999* meant that when entities were required under federal law to give information in writing, provide a signature or produce a document, they could do it electronically. However, the Australian Government and state and territory governments exempted a large volume of legislation from the operation of the Act. While the Act was an enabler, it didn't create a 'unique and un-forgeable identifier that can be checked by the receiver to verify authenticity and integrity and provide for non-repudiation'.<sup>10</sup>

At the end of the 1990s, the Department of Communications, Information Technology and the Arts was a central player in the coordination of e-government. Two units were created within the department: the Office for Government Online and the National Office for the Information Economy (NOIE), which provided advice and support to the government on internet-specific matters.<sup>11</sup> Some of the functions of the NOIE were subsequently taken over by the Australian Government Information Management Office, which was established in April 2004.

However, government departments and agencies had variable reputations, and innovative cross-government projects usually originated from the biggest departments.<sup>12</sup> To an extent, that's still the case, but with more coordination. In general, the major electronic players (such as the Tax Office and Centrelink) and innovative state governments were leading the field, advising central agencies and driving central initiatives.<sup>13</sup>

In 2016, the federal government established a new agency to manage the government's digital and ICT agendas: the Digital Transformation Agency (the successor to the Digital Transformation Office, launched in 2015). The agency aims to integrate digital delivery across the federal government and also enhance the transparency of the government's ICT and digital projects. It covers strategic and policy leadership on whole-of-government and shared ICT and digital service delivery, including ICT procurement policy.<sup>14</sup> The Digital Transformation Agenda, coordinated by the agency, foresees agencies and departments delivering 'a range of initiatives that will provide benefits to all users and improve their digital experience', including Single Touch Payroll; My Health Record; health payments; trusted digital authentication and verification; whole-of-government platforms; grants administration; and a streamlined online business registration service.<sup>15</sup> The Trusted Digital Identity Framework outlines a consistent approach to digital identity in Australia and will be an important component of any integrated approach to e-government.<sup>16</sup> Some \$92.4 million in funding was secured in the 2018–19 federal budget<sup>17</sup> to create the infrastructure that will underpin an eID (Govpass), and the government is aiming to roll out pilot services to half a million users by the end of June 2019.<sup>18</sup> This will largely duplicate an eID recently launched by Australia Post called Digital iD. The challenges to the widespread roll-out and adoption of eID in Australia are dealt with in a previous Policy Brief.<sup>19</sup>

States and local councils also deliver a range of services online. A leading actor is the New South Wales Government, which offers a single sign-on service for secure access to government transactions; more than 1.5 million customers have already signed up.<sup>20</sup> Victoria is another leader. In May 2016, it released the Victorian Government Information Technology Strategy, which outlines steps the government is taking to improve the security of information and infrastructure critical to the proper functioning of e-government.

At the local government level, the City of Sydney is contributing to the open data movement by making accessible to the public an ever-growing range of data in a number of formats. The datasets provide information on environmental sustainability, transport, arts and culture, facilities, parks and more.<sup>21</sup> Opening up data facilitates the creation and management of open services for the private and community sectors, increases transparency and stimulates the economy. It also decreases the number of information requests and reduces administrative workload.

# An integrated approach to e-government in Australia

An integrated approach to e-government in Australia would require detailed consultations across all three tiers of government, and with business and the public. However, several principles derived from the experience of others can help frame the approach.

## The once-only principle

The once-only principle (OOP) is central to joined-up government. The EU addressed this in its eGovernment Action Plan 2016–2020, where the foundations for the EU Digital OOP are laid out.<sup>22</sup> The OOP requires that individuals and businesses shouldn't have to supply the same information more than once to public entities (for example, when notifying a change of address). This requires the existence of public-sector interoperability at different levels: organisational, legal and technical. The conceptual model of the new European Interoperability Framework foresees interoperability levels as integral parts of integrated public service governance, meaning that different public administrations work together to meet citizens' needs and provide public services in a seamless way.<sup>23</sup>

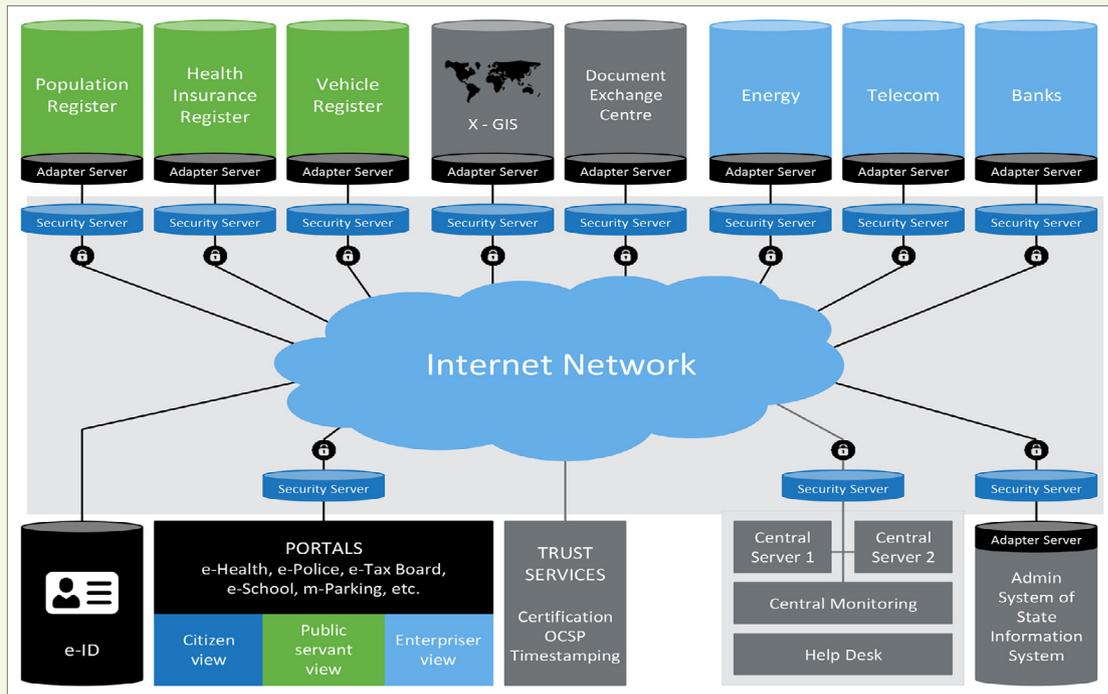
## A decentralised approach

Facilitating secure data exchanges and interoperability between different government agencies doesn't require the creation of a single database (a so-called superdatabase) that consolidates all data from other databases. In fact, doing that poses serious security risks. A decentralised approach enables different databases and IT solutions in the three tiers of government to 'talk' to each other securely and solves the problem of how to integrate the myriad different government databases and systems that already exist. Four key elements underpin this secure exchange:

- the identification of both the sender and the receiver of the data
- the encryption of data exchanged to ensure the data is unreadable in case someone intercepts it
- the time stamping of data transactions
- a legal audit trail via archiving and logging of electronic records.

In Estonia, X-Road (Figure 1) is a distributed information exchange platform that makes it possible for different systems to communicate across the entire governmental sector.<sup>24</sup>

Figure 1: Estonia's X-Road



Source: eGovernance Academy

## A digital identity

Digital identity is central to e-government. It serves two main functions: proving one's identity in the virtual space and verifying virtual transactions. Given the administrative division of Australia into six states and two territories, specific cross-border solutions promise added efficiencies. The EU has taken steps in the direction of cross-border electronic identification and trust services. Its eIDAS Regulation (no. 910/2014) ensures that people and businesses are able to use their own national eID schemes to access public services in other EU countries where such schemes are available. It also ensures the legal validity of digital interactions; that is, they have the same legal status as traditional paper-based transactions. The EU case highlights the need to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. With Australia Post's Digital iD and Govpass, Australia is laying the foundation for a national eID, although some major questions remain to be addressed.

## Privacy

Addressing privacy concerns through a citizen-driven e-government model is important in winning public support for integrated e-government, especially given the history of the failed Australia Card and scandals such as eCensus. Mutual trust is the key to interactions in which the government collects information about citizens and citizens provide their own data to the government. The principles of confidentiality, integrity and accessibility of data are all critical. Building trust between citizens and authorities is at the core of a working e-government model, so considerable emphasis should be put on communicating with citizens about how and for what reason their data will be processed by the government.

One lesson learned from abroad is the value of placing citizens in the driving seat. In Estonia, for example, every time a citizen's personal data is accessed by a government agency, the individual user can see that access via a log and contest it if they believe it to be improper. Another example from Estonia is related to the right to choose whether to use digital identity or not. Those who do not want to use their digital identity can still use a physical service centre. Australia is also planning an opt-in approach to its new digital identity; however, it may become de facto compulsory if private-sector organisations are able to insist as a condition of service that it's used (for example, to use online banking). Were that to eventuate, it would raise concerns about anonymity and the ability to not share information.

### **A joined-up back office**

In order to provide easily accessible e-government services across all tiers of government, a joined-up back office is central. So far, the success of some major agencies, such as the Tax Office and Centrelink, depends more on a joined-up 'front-end' (the interface between the user and the back office). As Catherine Garner has noted: 'Improving Australia's cross-agency collaboration and integration will provide efficient, dynamic systems with greater personalisation and support Australia on its journey to become an e-government leader'.<sup>25</sup>

### **Evaluating outcomes from government-funded services**

The ability to evaluate outcomes of publicly funded services is an important means of measuring the effectiveness of the government services being provided to citizens. Applying strict privacy and information security practices, there would be value in evaluating outcomes from government spending at the population level, rather than on a simple agency-by-agency basis. There would be community benefits in having the secure, de-identified evidence base made available for approved service improvement and evaluation of government-funded programs and policies.

### **Other issues**

In addition to these guiding principles, Australia will need to resolve a number of other important issues. In summary, they include the need to:

- ensure secure data exchange and security of data
- manage the integration process and metadata related to systems and services (a clearly defined and regulated approval process, for example via the Office of the Australian Information Commissioner, is needed for adding new components or new services to ensure smooth integration and the maintenance of security and privacy standards)
- ensure the right of all citizens using e-government services to easily access information about how government is using their data
- ensure the right of citizens to decide who can access their data
- ensure the right of citizens to decide whether or not to use their eID.

## Lessons learned from abroad

To implement integrated e-government in Australia, work is needed at several organisational, legislative and technical levels. A few conceptual questions were important when Estonia was developing integrated e-government:

- The question of how *to identify people, businesses and real estate* had to be addressed. In order to enable trustable and secure data exchanges between different databases and information systems, some identifiers for people, businesses and cadastral units are needed. In Estonia, ID numbers of people and businesses and also cadastral numbers are regulated by law and implemented in all databases and information systems. This is the precondition for secure and trustable data exchanges between different systems.
- *The digital ID and digital signature are issued by the same process.*<sup>26</sup> Private keys (for use by the public key infrastructure) are generated by crypto-processor (chip) and aren't downloadable.<sup>27</sup> The eID and digital signature constitute a part of the government-issued and guaranteed infrastructure, which is used by both the private and the public sectors.
- While an eID is obligatory if a citizen wants to use e-government services, the citizen *isn't* obliged to use their digital identity (they can use non-eID-based systems if they prefer).
- Finally, *the citizen is the owner of their own data.*<sup>28</sup> They can control the use of the data managed by the government. The use of personal data is strictly regulated by law. Everyone can restrict the use of their data by blocking access to it if the law doesn't specify otherwise.

Another lesson from Estonia concerns back-office integration. Several conceptual agreements underpinned the design of the country's e-government architecture:

- *Decentralisation:* The system is decentralised. There's no single point of failure, and the central management of the system doesn't 'see' the data, but only whether the system is working.
- *Ease of implementation:* The system should be easy to implement. Government institutions shouldn't need to change their existing systems and processes. Training on the integration of the systems should be offered to all technical experts working in e-government back offices.
- *Neutrality of technology platforms:* The integration of systems doesn't mean that all technical systems use the same platform. Usually, governments use a range of proprietary software platforms as well as open-source solutions and technologies developed by different vendors. Integrated e-government should accommodate those variances.<sup>29</sup>
- *Security of transactions:* Integrity, confidentiality and non-repudiation (the assurance that a party to a contract or a communication can't deny the authenticity of their signature on a document or the sending of a message that originated from them) should be guaranteed.<sup>30</sup>
- *Security of data and services:* Data and services should be secured so they can be transferred via public networks. The use of the public internet should be enabled, and the development of separate (usually very expensive) government data networks should be avoided.
- *Agile planning and implementation:* It's necessary to avoid large, complex projects and instead develop a comprehensive general architecture that can be divided into small components, while still giving due consideration to security requirements.

Of course, all countries are different. In every case, detailed analysis is needed and copy-paste solutions aren't possible. While the technical complexity of a solution is approximately the same in small and big countries, the main difference, and usually also the main challenge, lies in the organisational, legislative and change-management fields.

## Recommendations

We make the following recommendations for the further development of e-government in Australia.

- Avoid large e-government projects. Agile development can minimise risks, enable faster results and avoid implementation challenges.
- Establish a properly functioning secure eID and digital signature for each citizen. The eID should be simple and user-friendly, issued by government (similarly to passports) and guaranteed by law. It should be used for both e-government services and business e-services.
- Back-office integration should be coordinated centrally but done in a decentralised way, enabling secure data exchange between systems connected via the internet. The integration platform should enable the integration of different technical platforms in different locations, in different legal environments and with different organisational set-ups. The integration platform should be as simple as possible and not require changes to existing back-office processes and systems. Process redesign can be done step by step.
- A citizen-centric model is important to win public support for integrated e-government. It should allow people to control their private data and provide legal guarantees, supported by organisational and technical frameworks. Building trust takes time, so carefully planned communication between the government and citizens is critical, including building up and publicising a track record of competent and secure service delivery. This can be assisted by following basic design concepts and data protection principles when designing the eID and the back-office integration of IT systems.

Integrated e-government offers major benefits to businesses and citizens. It reduces the time and costs associated with transacting with government and with each other and makes life easier. A thoughtful approach to designing integrated e-government (such as decentralisation) will also mean that the risks of a data breach won't be increased. Australia's geography and population size don't present any technical obstacles to rolling out a world-class e-government system.

The move to create digital identities in Australia also suggests growing political momentum to take a more holistic approach to e-government. If it's citizen-centric, it could help win public support, too.

## Notes

- 1 The online sophistication ranking assesses service delivery against a five-stage maturity model: information; one-way interaction; two-way interaction; transaction; and targeting/automation. The fourth and fifth stages can be referred to as 'full online availability'. For more information, see Capgemini, IDC, Rand Europe, Sogeti, DTI, *Digitizing public services in Europe: putting ambition into action, 9th benchmark measurement*, report for the European Commission, December 2010, [online](#).
- 2 The release of the South Australian Government's digital driver's licence is a useful case study, highlighting what's possible, but also the critical missing piece for nationally consistent electronic identity and digital signatures, which inhibits the flourishing of e-services. See Department of Planning, Transport and Infrastructure, *South Australian driver's licences to go digital*, South Australian Government, 22 September 2017, [online](#).
- 3 Charlemagne, 'Estonia is trying to convert the EU to its digital creed', *The Economist*, 6 July 2017, [online](#).
- 4 Along with the Australian Computer Society, both the NSW and Victorian governments contributed funding towards this research and the visit to Australia by Dr Arvo Ott.
- 5 P Chen, RK Gibson, W Lusoli, SJ Ward, 'Australian governments and online communication', in S Young (ed.), *Australian government communication*, Cambridge University Press, Cambridge, 2007.
- 6 The Australian Management Advisory Committee's 2004 *Connecting government* report defined the concept of whole-of-government in the Australian Public Service as follows: 'Whole-of-government denotes public services agencies working across portfolio boundaries to achieve a shared goal and an integrated government response to particular issues. Approaches can be formal or informal. They can focus on policy development, program management, and service delivery.'
- 7 P Dunleavy, H Margetts, S Bastow, J Tinkler, 'Australian e-government in comparative perspective', *Australian Journal of Political Science*, 2008, 43(1):13–26, [online](#).
- 8 G Greenleaf, 'The Australia Card: towards a national surveillance system', *Law Society Journal*, 1987, 25(9), [online](#); R Clarke, 'Just another piece of plastic for your wallet: the "Australia Card" scheme', *Prometheus*, 1987, 5(1):29–45.
- 9 Office of the Access Card, *How will the card benefit you?*, Australian Government, no date, [online](#).
- 10 Attorney-General's Department, *The Electronic Transactions Act 1999*, information sheet, no date, [online](#).
- 11 Also, in 1997 the new Liberal–National government launched a major central government outsourcing initiative in order to improve private-sector involvement in government. The aim was to outsource IT across the whole federal government. All departments and agencies were forced to outsource their IT operations to one of the largest international IT corporations with an Australian presence. In 2001, following critical reports from the Australian National Audit Office, the initiative was replaced by more conventional procurement methods. However, the same contractors continued to be important players, consolidating the IT market and leaving little expertise within the government, except for the largest departments. See Dunleavy et al., 'Australian e-government in comparative perspective'.
- 12 For instance, the Australian Taxation Office enables individual taxpayers and their agents to use the 'e-Tax' electronic tax return lodgement facility to prepopulate their tax returns with data provided through Medicare Australia and Centrelink. Dunleavy et al., 'Australian e-government in comparative perspective'.
- 13 Dunleavy et al., 'Australian e-government in comparative perspective'.
- 14 Eden Estopace, 'Australia creates new digital agency to oversee government's ICT projects', *EGov Innovation*, 1 January 2016, [online](#).
- 15 Digital Transformation Agency (DTA), 'Whole-of-government transformation vision', in *Digital Transformation Agenda*, Australian Government, no date, [online](#).
- 16 DTA, 'Consultation', in *Trusted Digital Identity Framework*, [online](#).
- 17 Australian Government, *Budget 2018–19*, Budget paper no. 1, 1–22, [online](#).
- 18 Michael Keenan, 'Delivering Australia's digital future', transcript, 13 June 2018, [online](#).
- 19 Fergus Hanson, *Preventing another Australia Card fail: unlocking the potential of digital identity*, ASPI ICPC, October 2018, [online](#).
- 20 Ping Identity 'More than 3 million sign up to NSW's unified SSO portal', 2018, [online](#).
- 21 City of Sydney, City of Sydney open data portal, [online](#).
- 22 European Commission, *EU-wide digital once-only principle for citizens and businesses: policy options and their impacts*, 1 February 2017, [online](#).
- 23 European Commission, *The new European Interoperability Framework*, 13 July 2018, [online](#). The DTA also has a 'tell us once' principle; DTA, *Digital Transformation Agenda*, [online](#).
- 24 For more information about X-Road in Estonia, see Information System Authority, *Data Exchange Layer X-Road*, Republic of Estonia, 21 February 2017, [online](#); and 'X-Road', *Cybernetica*, [online](#). One video on e-Estonia is 'Living in a digital society: e-Estonia', *YouTube*, 21 May 2015, [online](#).
- 25 Catherine Garner, 'Can Australia lead the world in e-government?', *The Canberra Times*, 27 September 2016, [online](#).
- 26 More information on eID in Estonia is accessible at *ID*, [online](#); and 'Estonian e-identity corner stone: state issued national ID card', *YouTube*, 10 July 2013, [online](#).
- 27 Key generation is performed on the user's card and not by a central facility.
- 28 Under the Archives Act, all data and information held by the government is owned by the government. Intellectual property may be owned by the originator of the data, but not the object within which it's contained. Legislative changes are in train to expand the definition so that it isn't just property based. Legal dilemmas beyond the scope of this paper include whether access approval can be separate from ownership and how far that extends. Another is what happens to and who owns personal data if someone dies.
- 29 Integrated e-government inherently presents a large and attractive target for attack. To mitigate this the basic systems participating as servers in this environment must meet ASD EPL levels of security compliance, preferably at EAL4+ and OSLSP. OSLSP enables full separation of data/processes with high trust.
- 30 For some systems, such as those using Windows XP, this wouldn't be possible to guarantee.

# Acronyms and abbreviations

- eID digital identity
- GDP gross domestic product
- IC information and communications technology
- IT information technology
- NOIE National Office for the Information Economy
- OOP once-only principle

## Some previous ICPC publications

