Interoperability Technical Framework for the Australian Government

June 2003
Interoperability Technical Framework for the Australian Government

June 2003

ISBN (print)    1 74082 015 0
ISBN (online)   1 74082 016 9

© Commonwealth of Australia 2003

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without the prior written permission from the Commonwealth.

Requests and inquiries concerning reproduction and rights in this publication should be addressed to:

Manager, Public Affairs
National Office for the Information Economy
GPO Box 390
Canberra ACT 2601
Australia is currently immersed in transforming the way it delivers services and manages regulatory processes and compliance for citizens, business and communities. Government agencies are working more closely together, taking a whole of government approach to service delivery. The ability to manage information effectively and co-ordinate disparate data sources will be key enablers of this process. The use of information technology to achieve these ends is now referred to as e-government.

Interoperability, or enabling seamless connections, is fundamental to achieving Australia’s e-government aims. The whole of government approach we are taking requires a foundation of common standards and enablers. These facilitate cooperation and collaboration across Australian governments, as well as the community and business sectors.

The Interoperability Technical Framework for the Australian Government has been developed by the National Office for the Information Economy (NOIE) and a reference group of senior technical architects drawn from key government agencies. It responds to developments in the Information and Communications Technology (ICT) industry driving business and government in the direction of interoperability and interconnectedness. Its development has also evolved from a number of industry workshops on interoperability held in 2002, as well as consultation with the Australian Information Industry Association.

The Framework specifies agreed technical standards that will enable Australian Government ICT systems to communicate and exchange information. The demands of customer-focused service delivery mean government and private sector business operations increasingly intersect. The adoption of common technical protocols and standards will ensure that Government ICT systems interoperate in a trusted way with partners from industry and other governments. Achieving interoperability will improve efficiency, reduce costs to business and government and will enhance government agencies’ capacity to respond to public policy developments.

The Framework represents one of the first steps in developing an online environment where government services are integrated to better serve the needs of business and the community at large. These also provide the means for both government and business ICT systems to communicate and transact.

The Framework exists in recognition that interoperability will develop from a starting point of independent ‘siloed’ environments using different systems, but with a common business need - to exchange data. This framework establishes agreed technical standards but to achieve the wider goals of e-government will require framework agreements around governance, legal, financing and business interoperability.

While it provides an initial structure upon which to build interoperable systems, the Framework will operate as a living document and will continue to develop as improvements and changes in technical, business and administrative processes emerge. The Chief Information Officer Committee (CIOC) has resolved to review the Framework on an annual basis while taking advantage of opportunities as they arise. This review will be a consultative process managed by nominated representatives of the CIOC. This group will maintain the Framework to be responsive to ICT industry trends and agency needs. NOIE will facilitate this process and provide better practise guidance to agencies.

John Rimmer
Chair, Chief Information Officer Committee
May 2003
Table of Contents

PREFACE iv

1. INTRODUCTION 1

2. INTEROPERABILITY TECHNICAL FRAMEWORK OVERVIEW 4

   2.1 Principles 4
   2.2 Chief Information Officers’ role 4
   2.2.1 Developing the Framework 4
   2.2.2 Implementing the Framework in your Agency 5
   2.2.3 Contributing to the Framework between agencies 5
   2.3 National Office for the Information Economy (NOIE) role 5
   2.4 Further Development of the Framework 6
   2.5 Measures of success 6

3. THE FRAMEWORK: POLICIES AND STANDARDS 8

   3.1 Policies for data and interconnection 8
   3.2 List of standards covered by this Framework 9

4. CONCLUSION 12

APPENDIX A 13

GLOSSARY 14

**CIOC**

CHIEF INFORMATION OFFICER COMMITTEE

CIO COMMITTEE
The CIO Committee (CIOC) reports to the Information Management Strategy Committee (IMSC), which provides shared leadership on multi-agency and whole-of-government information management strategies. The CIOC identifies strategic issues, addresses issues referred by the IMSC and develops options for adoption and implementation of Information and Communications Technology (ICT) at agency or whole-of-government level. The CIOC comprises representatives from 25 agencies and is chaired by Mr John Rimmer, the CEO of the National Office for the Information Economy. Its membership is drawn from both key central agencies and agencies that are high users of ICT. Through working groups, it is addressing specific issues and promoting research and development and knowledge sharing.
Preface

Members of the Interoperability Framework Working Group:

- **Jed Bartlett**, Office of the Chief Information Officer, Department of Defence;
- **Don Bartley**, Director, Technology Research Branch, Australian Bureau of Statistics;
- **Steve Crisp**, National Manager, Enterprise Architecture-Applications, Centrelink;
- **Kevin Fiebig**, Director, Strategy and Coordination, Department of Family and Community Services;
- **Thomas Schild**, Business Systems Architect, Business Solutions Group, Department of Immigration and Multicultural and Indigenous Affairs; and
- **Brian Stonebridge**, Interoperability, Business Strategies Branch, National Office for the Information Economy.

We believe that interoperability between agencies for the exchange of data and services is an important cornerstone for improving Government business operations. This draft of the Interoperability Framework for the Australian Government represents a collaborative effort by representatives of a number of agencies.

The draft Interoperability Framework is a starting point in managing future Information and Communication Technologies investment strategies on behalf of government. Increasingly the process for obtaining Information Technology and Information Management investment funds will come under greater scrutiny. The ability to show future benefits in terms of interoperability will be an advantage in demonstrating an effective return on investment.

We commend the Interoperability Framework for the Australian Government to you, and seek your acceptance of this foundation stone and your active participation in enriching the Framework over time.

Available from:

For further information contact:
Brian Stonebridge, brian.stonebridge@noie.gov.au
02 6271 1086
Australian governments are actively pursuing the opportunities presented by technological developments to maximise government performance. Governments across all jurisdictions are transforming the way they work and the ways in which they deliver services. A key part of this transformation is the integration of service delivery through multiple channels in a way that focuses on citizens’ needs. The Prime Minister increasingly requires consideration of whole of government issues in new policy making. Government policies and programs for citizens, business and communities are being developed and delivered across more than one agency. These include the Australians Working Together initiative, business registration, and the streamlining of common services such as the administration of community grants. In response to this changing environment governments around the world are developing technical frameworks to enable more efficient and effective operations.

The annual Australian Government expenditure on Information and Communications Technology (ICT) is estimated at $3.5 billion ($2.1 billion recurrent and up to $1.4 billion capital). The government has a significant and rapidly growing investment in electronic information management and service delivery. Citizens’ expectations, demands for better service delivery and anticipated efficiency gains are key drivers of this growing investment.

Australian governments are reaping the benefits of improved service delivery outcomes, greater efficiency and reduced duplication. The Australian Government has recognised the opportunities in this area and has established a governance framework which provides the key elements of a coordinated, whole of government approach to e-government. This approach ensures that specific Australian Government agencies retain responsibility and accountability for outcomes and promotes flexibility in response to both changes in the environment and emerging customer needs. This federated interoperability environment will protect the major investment in ICT by extending the life of current systems and enabling more efficient transitions between systems in the future.

Ultimately, collaboration between agencies to deliver more efficient and effective government, will require harmonization of policy, legal and business environments across agencies and jurisdictions. The Interoperability Technical Framework for the Australian Government provides the first step in establishing this environment at the technical level for the exchange of data and harmonization of business transactions within a trusted environment. It is a basic foundation, and will be a living, breathing framework that will grow over time.

---

**Interoperability** is defined as the ability to transfer and use information in a uniform and efficient manner across multiple organisations and information technology systems. It underpins the level of benefits accruing to enterprises, government and the wider economy through e-commerce.

**A Framework** is an overarching set of policies, standards and guidelines which define the way agencies have agreed to do business with each other at a point in time; but is adaptable as technologies, standards and agency needs change.

**Australian Government** agencies will become part of the Framework through endorsement by their Chief Information Officer or equivalent.

---


Each agency will have its own vision of how it will interact with its customers and other agencies over coming years. Interoperability is concerned with the “dialogue” between agencies. Agencies’ own business drivers will influence their progress towards interoperability. Many agencies already have an internal interoperability framework in place – the role of this framework is to provide coherence in this dialogue across agencies. When agencies and governments across the three tiers of government talk to each other, they must do so securely and in a commonly understood language. A coherent framework of interoperability also lays the basis for government to present a consistent face to its citizens and customers.

Perhaps the best way to understand what a successful Interoperability Technical Framework could mean in the future is to do a little crystal ball gazing, jumping ahead to the year 2005.

In 2002, J. Citizen is in the process of setting up a new business. In order to comply with local, state and federal legislation, the business owner must apply for and obtain numerous permits and licences. After obtaining an Australian Business Number (ABN), the business owner will use the business’ ABN on numerous application forms. It is a time consuming process for the three levels of government concerned who must manually verify the integrity of the ABN related data of the business concerned.

By 2005, ABPpublic have developed and implemented an XML interface for the ABN related business data accessible from the Business Entry Point’s portal. J. Citizen now has access to a convenient online registration process, which makes her business details available to all authorised users - no more filling in the same information on form after form.
Five years earlier, agencies would have had limited access to verify business details. Five years earlier a number of systems were maintained independently, with information provided to State and Local governments through a variety of manual methods. In 2005 one streamlined process puts J. Citizen in business - faster.

Interoperability will also facilitate more convenient access to government services through external service delivery agencies. An example of this is the NOVEL Veterans’ electronic lodgement service which was piloted in Tasmania through the TIGERS program. It is an online claim submission system with inbuilt “intelligent” support. It provides additional convenience of service points for the customer and an additional channel of online services, providing quicker, simpler and easier access to Veterans’ Affairs services. The online channel supports an extended reach physical customer support network via ServiceTasmania shopfronts and Ex-Service organisations.

The investment in developing and adhering to the Interoperability Technical Framework provides benefits in quality of service throughout the chain - from client through officer, agency, government - and therefore to the economy as a whole. For agencies the benefits of a robust, well-supported Interoperability system may include more rigorous decision making, less time wasted and better service for the client. Agencies will benefit from reduced risk and lead time in the development of collaborative programs. The agency and government enjoy more efficient operations, such as authorised access to more current and reliable data, reduced duplication and better service delivery to the customer; both more responsive and more efficient.

The Framework has been developed to be consistent with broader industry trends. A successful Interoperability Technical Framework requires the involvement of all government Chief Information Officers. This means a strong commitment to collaboration and it means creating a cultural network that operates beyond internal systems. Crucially, this Framework will only be effective if agencies and departments support it and use it.
2.1 PRINCIPLES
This Framework provides a high level or minimum basis for interoperability within government. It informs the Australian Government level in the figure below. It is a business requirement for agency systems to interoperate with other agency systems, other jurisdictions and broader stakeholders such as private sector service providers. Figure 2 illustrates the relationship between the spheres of government, industry and the wider community. It is critical for the development of a truly interoperable environment supporting business and government functions, for government and business interoperability frameworks to be informed by each other and for their development to be undertaken in close consultation.

The following principles underlie the Framework:

- Agencies agree to collaborate within a federated model to achieve flexibility in the delivery of programs and services, in ways that achieve government objectives and meet the needs and circumstances of citizens;
- Government Interoperability draws on established standards and recognises the opportunities provided by ICT industry trends;
- Existing Australian and international standards will be adopted wherever available and appropriate;
- This Framework is open standards based, that is all standards and guidelines must conform with open standards principles;
- Interoperability will be based on a trusted, secure framework;
- The Framework will adapt to changing requirements over time and will be maintained at a strategic level; and
- Agencies will work within relevant industry sectors and communities of interest to determine the appropriate level of interoperability to meet the requirements of their agency, sector or community.

For example, participating in harmonization of the grants administration process across agencies also offers agencies opportunities to gain efficiencies internally.

2.2 CHIEF INFORMATION OFFICERS’ ROLE
Chief Information Officers (CIOs) are vital to the development and implementation of this Framework. This section outlines the role of CIOs and agencies in relation to interoperability.

2.2.1 DEVELOPING THE FRAMEWORK
This Framework was developed through extensive consultation. A first draft of the ‘Interoperability Framework’ was developed within NOIE and was
primarily informed by the efforts of the United Kingdom e-Envoy in developing the UK Government Interoperability Framework (eGIF)\(^1\) and knowledge of the standards already used or commonly accepted within Australian Government agencies.

It was reviewed by the 'Interoperability Framework Working Group' operating as a loose sub-committee of the Commonwealth Architecture Forum, a coalition of architects working in Australian Government agencies. This working group was instrumental in providing technical advice and direction to the Interoperability Technical Framework. It was also circulated to representatives of the ICT industry (the Australian Information Industry Association), State, Territory and Local governments. The comments made by the working group and as a result of the wider circulation were incorporated in the second draft, which formed the basis for formal consultation. This second draft was circulated widely within the Australian Government to inform Chief Information Officers and other interested senior officers about the proposed Interoperability Technical Framework, to seek their comments on the draft Framework and to commence the process of seeking their on-going commitment to implementing and extending the Framework.

The valuable input and endorsement provided by these officers has informed this paper, the Interoperability Technical Framework for the Australian Government (the Framework). The Information Management Steering Committee (IMSC) Commonwealth Chief Information Officer Committee (CIOC) has endorsed Version 1 of the Framework.

Version 1 of the agreed Interoperability Technical Framework for the Australian Government will be accessible through the NOIE website.

2.2.2 IMPLEMENTING THE FRAMEWORK IN YOUR AGENCY

Chief Information Officers are primarily responsible for the success of the Framework. Interoperability depends as much on a culture of collaboration within and between agencies, as it does on the consistent use of agreed standards.

CIOs can implement the Framework within their agency by endorsing it as agency policy and ensuring it is referenced in relevant agency policies. A CIO may use the opportunity to rationalise processes, as a result of increased interoperability, to improve the quality of services and to reduce the cost of service provision. Naturally implementation will happen over time as systems reach the end of their life cycle. CIOs who have committed to implementing this Framework may engage in activities that:

- Raise awareness of the Framework within the agency;
- Adopt the Framework as a guide to agency policy;
- Ensure it is used appropriately, for example as business systems are ready for replacement consider the relevance of interoperability; and
- Create an environment for officers to raise and action interoperability issues.

CIOs can support the aims of the Framework by ensuring the following business rules operate within their agency, within the context of existing agency policy:

- Trust, including privacy and a level of authentication appropriate to the particular service, and sensitivity of information; and all risks are identified and managed appropriately within the agency;
- Security issues are identified and managed appropriately within the agency; and
- Data quality and integrity is managed appropriately within the agency, and on the premise that information content may at some time be transferred across agency boundaries.

Participation in the Framework will help agencies take advantage of cross agency services such as the Business Authentication Framework; which will provide trust, privacy and authentication.

2.2.3 CONTRIBUTING TO THE FRAMEWORK BETWEEN AGENCIES

CIOs play an important role in the continuous development and improvement of this Framework by:

- Ensuring the agency can interoperate with other agencies, by using the Framework for services that involve data exchange with other agencies;
- Participating in the processes to develop the Framework, standards and XML schema.

2.3 NATIONAL OFFICE FOR THE INFORMATION ECONOMY (NOIE) ROLE

This Framework has been developed in close consultation with key Australian Government agencies. CIOC has set the strategic direction and through

\(^1\) http://www.govtalk.gov.uk
consultation and their endorsement the Framework is collectively owned by CIOs. NOIE’s role is to guide agencies along this path.

NOIE will act as the focal point for facilitating the Framework and the provision of agreed XML schema for use throughout government.

2.4 FURTHER DEVELOPMENT OF THE FRAMEWORK

This Framework will be reviewed annually to ensure consistency with national and international developments.

It is anticipated that an early priority will be the development of an online repository to support the Framework. It will be the vehicle for the web publication of the Interoperability Technical Framework, a key communication channel for agencies developing the Framework further, and the mechanism for sharing XML schema. Opportunities exist for this repository to be scoped, developed populated and used by the public and the private sector.

Other potential priority areas for development, identified through consultations to date, include:

- Identify which common business processes need standards and XML schema development;
- Set the specifications for, and coordinate the production of, XML schema for use across government; and

- Develop standards and XML schema in consultation with agencies.

Other issues that might be considered are:

- Embedding interoperability concepts in other technical frameworks, such as authentication frameworks, procurement frameworks, frameworks for specific sectors and frameworks for specific communities of interest;
- Directory system interoperability;
- Network interoperability issues;
- Web service security;
- Non text data such as voice, graphics, sound, video images;
- Redesign of business processes so that they can benefit from online delivery:
  - how business rules are applied to integrated services;
  - how trust and risk are handled across organisational boundaries; and
- Integration in the context of outsourced environments.

2.5 MEASURES OF SUCCESS

CIOs shall consider the Interoperability Technical Framework to be successful when:

For the CIO - The CIO or appropriate delegate of CEO has signed the Framework as part of agency policy, and the Framework is referenced in relevant internal agency frameworks such as the agency enterprise architecture, ICT strategy, online action plans; the Framework is referenced and used in all relevant government ICT procurement activities; all relevant security and privacy considerations associated with implementing the Framework have been appropriately addressed and managed; and staff are aware of the Framework and use it in appropriate situations.

For the Agency - Measures of success include the development of an agency framework for interoperability encompassing the Interoperability Technical Framework, the agency is contributing resources to develop the Framework, and the agency is successfully interoperating in a trusted manner with other agencies based on the standards in the Framework.

For the Australian Government - Measures of success include increased awareness of the Framework and interoperability issues, referencing of the Framework by related frameworks; agencies find it easier to interoperate through use of the Framework standards, resulting in more efficient government business operations.

For the community - The true measure of success will be that the Framework operates as a key enabler for the development of integrated services; which in turn enable better service provision, to government clients, business and the wider community.
This section defines policies and standards needed to achieve interoperability and seamless information flows across government. This Framework builds on the standards established by the Government Online Strategy 2 in April 2000, operates within the context of other frameworks, and will shape other frameworks. “Interoperability” is deliberately defined in a narrow way for this version. At a high level the policies and standards which allow electronic information and transactions to interoperate across government relate to the areas of Security, Interconnection, Data exchange and Web service integration.

The Australian Government protective security framework is well established, as described in the Australian Government Protective Security Manual (PSM) issued by the Attorney General’s Department. The other key policies that will enable greater “interconnectivity” and “data exchange” are making the best use of the Internet, the adoption of XML as the primary standard for data exchange, and the adoption of the “web services” model. The web browser is the key human interface for access to online services. Making the best possible use of the Internet entails the universal adoption of common specifications used on the Internet and World Wide Web for all public sector information systems. Data exchange will be achieved through the development of common XML schema based on existing Australian standards where appropriate. The web services model uses XML, SOAP/XMLP, WSDL and UDDI for service integration.

Let’s pick up the story of J. Citizen, when a web services enabled business register is available across government, to illustrate how this model could work. As previously mentioned, by 2005 ABRpublic have developed and implemented an XML interface for the ABN related business data accessible from the Business Entry Point portal. This is accessible for querying by authorised persons and via a web service.

Today a manual interface to ABN data is available, via the web or various batch media. By 2005 the web service interface has provided an interoperable format for data to be passed between government agencies. When local, state and federal government agencies process business applications, the time consuming processes of manually searching for and verifying ABN-related data are carried out automatically, machine to machine, without manual intervention.

This exchange of organisation data is supported by XML schema for businesses based on Australian standards such as the standard for interchange of client data (AS4590). Use of shared XML schema allows integration of data from multiple sources.

Interconnectivity is provided through the use of common SOAP (XMLP) messaging over Internet protocols. For example a small Australian Government agency links into this service via Fedlink, a secure VPN. A large State agency has a secure direct connection, operating over MQ series. Government’s shared use of XML schema, across the whole of government, facilitates the immediate processing of data, subject to appropriate security and privacy considerations.

3.1 POLICIES FOR DATA AND INTERCONNECTION
This Framework draws on and incorporates key previously established policies for data definition and protection and for systems interconnection, as defined below:

**Security:** The Australian Government Protective Security Manual (PSM) issued by the Attorney General’s Department. It is the principal means for disseminating Australian Government protective security policies, principles, standards and procedures to be followed by all Australian Government agencies for the protection of official resources. The PSM is the Australian Government’s top-level framework for physical, information and personnel security. An outline is available at [http://wwwag.govau/www/protectivesecurityHome.nsf](http://wwwag.govau/www/protectivesecurityHome.nsf).


Between Australian Government agencies, where connection is over the Internet, the use of Fedlink ([http://wwwfedlink.govau/](http://wwwfedlink.govau/)) encryption routers will ensure confidentiality.


**Privacy:** Australian Government agencies are bound by a regulatory framework, administered by the Office of the Federal Privacy Commissioner. A recent paper (Privacy in Australia – October 2001) ([http://wwwprivacy.govau/publications/pia1.html](http://wwwprivacy.govau/publications/pia1.html)) has an overview of privacy regulation in Australia, and covers some of the important privacy issues in Australia.


**Data definition:** Policy is to use existing standards - where formal Australian standards exist (such as the Australian standard for interchange of client information (AS4590), the Australian Government Locator Service [http://wwwnoie.govau/projects/egovernment/better%5Fpractice/agls.htm](http://wwwnoie.govau/projects/egovernment/better%5Fpractice/agls.htm) for metadata) they should be used, or if considered not exactly suitable, then steps taken to update the standard.

**Government Domain Naming:** The policy is set by the Online Council and managed by National Office for the Information Economy (NOIE) [http://wwwnoie.govau/projects/egovernment/better%5Finfrastructure/australiangovernmentdomainguidelines.htm](http://wwwnoie.govau/projects/egovernment/better%5Finfrastructure/australiangovernmentdomainguidelines.htm).
3.2 LIST OF STANDARDS COVERED BY THIS FRAMEWORK

The following section lists minimum standards to allow agencies to interoperate. This is not an exhaustive listing of all standards but identifies standards that will position the Australian Government for the future.

These standards allow seamless interconnection, resource discovery, data definition and exchange, and a model for the creation of interoperable services. Many are already in common use in Australian Government agencies.

3.2.1 STANDARDS OWNERS

The owners of the various standards listed are:

- **International:**
  - The Internet Engineering Task Force (IETF) http://www.ietf.org/rfc.html;
  - International Organisation for Standardisation (ISO) http://www.iso.org;
  - Open GIS Consortium (OGC) http://www.opengis.org;
  - World Wide Web consortium (W3C) http://www.w3.org;

- **National:**
  - Standards Australia; Online Council. Standards Australia http://wwwstandards.com.au3 has shown keen interest in working with government to define required standards. The Online Council operates as the peak ministerial forum across governments in Australia for consultation and coordination on the information economy http://wwwnoie.gov.au/projects/framework/coordination/onlin council.htm; and

- **Government:**
  - Attorney General’s Department http://wwwag.gov.au/;
  - Defence Signals Directorate (DSD) http://wwwcsd.gov.au;
  - National Archives of Australia (NAA) http://wwwnaa.gov.au;

---

**Figure 3: Interoperability by Service Layer**

<table>
<thead>
<tr>
<th>Service layer</th>
<th>Interoperability standard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Presentation</strong></td>
<td>to be developed, XSL.</td>
</tr>
<tr>
<td><strong>Business processes</strong></td>
<td>UML, WSDL, UDDI, SOAP, HTTP, HTTPS</td>
</tr>
<tr>
<td><strong>Specification discovery</strong></td>
<td>XSD, XSLT, eBXML, XML schema informed by existing standards, AS4590, AGILS</td>
</tr>
<tr>
<td><strong>Invocation security</strong></td>
<td>SOAP enabled middleware, TCP</td>
</tr>
<tr>
<td><strong>Data Content</strong></td>
<td>Various, including Internet Protocol</td>
</tr>
<tr>
<td><strong>Transport</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Security
These policies and standards provide a secure framework for interconnection and data exchange. Note: The DSD’s guide written in the context of interoperability is attached (Appendix A).

<table>
<thead>
<tr>
<th>Standards for:</th>
<th>Name of Standard</th>
<th>Status</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>For physical, information and personnel security policy</strong></td>
<td>Australian Government Protective Security Manual (PSM)</td>
<td>In use</td>
<td>Attorney General’s Department</td>
</tr>
<tr>
<td><strong>For information security systems</strong></td>
<td>Australian Communications-Electronic Security Instructions 33 (ACSI33)</td>
<td>In use</td>
<td>Defence Signals Directorate.</td>
</tr>
<tr>
<td><strong>For information security</strong></td>
<td>Information security management - Specification for information security management systems AS/NZS7799.2001 based on ISO 17799</td>
<td>In use</td>
<td>Standards Australia</td>
</tr>
<tr>
<td><strong>For risk management</strong></td>
<td>Risk management AS/NZS4360.1999</td>
<td>In use</td>
<td>Standards Australia</td>
</tr>
</tbody>
</table>

### Interconnection
These components and specifications are important to harmonise the technical level of data and service integration. Most are already in common use in Australian Government agencies. Note: Copies of the IETF RFCs can be found at http://www.ietf.org/rfc.html and W3C specifications can be found at http://www.w3.org/TR

<table>
<thead>
<tr>
<th>Standards for:</th>
<th>Name of Standard</th>
<th>Status</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>For Internet transport</strong></td>
<td>Hypertext transfer protocol HTTP (RFC 2616),HTTPS, TLS (RFC 2246), TCP/IP (RFC 793) and UDP (RFC 768) where required, subject to security constraints</td>
<td>In use</td>
<td>IETF</td>
</tr>
<tr>
<td><strong>For web services transport</strong></td>
<td>Simple Object Access Protocol (SOAP), XML Protocol (XMLP)</td>
<td>Developing</td>
<td>W3C</td>
</tr>
<tr>
<td><strong>For Government Domain Naming</strong></td>
<td>Domain Name System (DNS) (RFC 1035)</td>
<td>In use</td>
<td>IETF</td>
</tr>
<tr>
<td><strong>For Internet File transfer</strong></td>
<td>File transfer protocols FTP (RFC 959) with restart and recovery and HTTP (RFC 2616) for file transfer.</td>
<td>In use</td>
<td>IETF</td>
</tr>
<tr>
<td><strong>For e-mail</strong></td>
<td>SMTP/MIME/SMIME Multiple RFCs.</td>
<td>In use</td>
<td>IETF</td>
</tr>
<tr>
<td><strong>For Newsgroup services</strong></td>
<td>NNTP (RFC 977).</td>
<td>In use</td>
<td>IETF</td>
</tr>
</tbody>
</table>

### Discovery
These components and specifications are important to enable consistent discovery of information and services. Australian Government Locator Service (AGLS) metadata is in common use in Australian Government agencies. Note: Copies of the W3C specifications can be found at http://www.w3.org/TR

<table>
<thead>
<tr>
<th>Standards for:</th>
<th>Name of Standard</th>
<th>Status</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource discovery</strong></td>
<td>AGLS Metadata and extensions Australian Government guidelines</td>
<td>In use</td>
<td>NAA NOIE</td>
</tr>
<tr>
<td><strong>For web services discovery</strong></td>
<td>Web services model - see Glossary for explanation</td>
<td>Developing</td>
<td>W3C</td>
</tr>
<tr>
<td><strong>For web services directory</strong></td>
<td>Universal Description, Discovery and Integration (UDDI), <a href="http://www.uddi.org">http://www.uddi.org</a></td>
<td>Developing</td>
<td>W3C/ UDDI</td>
</tr>
<tr>
<td>Standards for:</td>
<td>Name of Standard</td>
<td>Status</td>
<td>Owner</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>Data exchange</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>These components and specifications are necessary to allow consistent definition, markup, presentation and exchange of information and services. Note: Copies of the W3C specifications can be found at: <a href="http://www.w3.org/TR">http://www.w3.org/TR</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For Metadata definition of data elements</td>
<td>Information technology — Specification and standardization of data elements Parts 1-6 (ISO 11179)</td>
<td>In use</td>
<td>ISO</td>
</tr>
<tr>
<td>For Data definition</td>
<td>Australian standards, eg Interchange of client information (AS4590) AGLS (see Resource discovery above)</td>
<td>In use</td>
<td>Standards Australia</td>
</tr>
<tr>
<td>For Vocabulary</td>
<td>AGIFT TAGS ABS classifications</td>
<td>In use</td>
<td>NAA NOIE ABS</td>
</tr>
<tr>
<td>For Web content</td>
<td>XML (Extensible Markup Language) meta language HTML</td>
<td>In use</td>
<td>W3C W3C/IETF</td>
</tr>
<tr>
<td>For Metadata definition of content</td>
<td>XML schema</td>
<td>In use/ Developing</td>
<td>W3C Agencies</td>
</tr>
<tr>
<td>For Geospatial data</td>
<td>GML (Geography Markup Language) <a href="http://www.opengis.org/techno/specs.htm">http://www.opengis.org/techno/specs.htm</a></td>
<td>Developing</td>
<td>Open GIS Consortium (OGC)</td>
</tr>
<tr>
<td>For Data transformation</td>
<td>XSL (Extensible Stylesheet Language)</td>
<td>In use/ Developing</td>
<td>W3C</td>
</tr>
<tr>
<td>For Data modelling and description</td>
<td>UML™ (Unified Modelling Language) RDF (Resource Description Framework)</td>
<td>Developing</td>
<td>W3C</td>
</tr>
<tr>
<td>For web services description</td>
<td>Web services Description Language (WSDL)</td>
<td>Developing</td>
<td>W3C</td>
</tr>
<tr>
<td>For character set</td>
<td>UNICODETransformation Format 8 bit UTF-8 <a href="http://www.unicode.org">http://www.unicode.org</a></td>
<td>In use</td>
<td>UNICODE IETF</td>
</tr>
</tbody>
</table>

Note: Generally where an Australian standard is based on an ISO standard the ISO standard is not referenced.
4. Conclusion

Through ongoing collaboration between government agencies led by Chief Information Officers we can achieve an environment where data can easily be exchanged between systems. This interoperability, as realised through this collaborative effort, underpins the level of benefits accruing to enterprises, government and the wider economy through e-commerce.

The adoption of common protocols and standards will help ensure that Australian Government IT services are interoperable with those of trading partners from industry and other governments. A commitment by Australian Government agencies to collaborate together and implement a shared Interoperability Technical Framework is an important foundation for initiatives such as the integration of services and development of e-business capability.
SECURITY CONSIDERATIONS.

Amongst others, the following list of security issues will have to be considered and addressed as part of implementing an interoperability framework:

1. The overall management processes/control mechanisms required that address the “big picture” issues of interoperability. For example:
   a. addressing the different standards and levels of security of the different stakeholders (Australian Government, State and Local governments, private industry and community sectors);
   b. defining and managing the relationships/levels of interoperability between the three tiers of government, industry and the community;
   c. the level and any restrictions on the classification/sensitivity of the information traversing the framework;
   d. defining and managing how the Interoperability Technical Framework fits into and supports other frameworks and identification and management of security issues associated with this;
   e. the security, business impact and cost implications of changing the standards/specifications and evolving/updating or changing the framework;
   f. defining and allocating responsibility for security;
   g. change control;
   h. legacy systems;
   i. proprietary issues;
   j. control and knowledge of who is authorised, and who is connecting to which resources (accountability/auditability);
   k. the impact of changes made by one stakeholder on the whole; and

2. other security issues such as the weakest link in the chain” potential security flaws;

2. Identification and management of the risks and threats associated with implementing the interoperability framework; and

3. Identification and implementation of a minimum set of security controls required to ensure availability, confidentiality, integrity, authenticity and non-repudiation of information traversing the framework is maintained and consistent with its classification/sensitivity. From the government perspective, this should be in line with government policies/requirements (e.g. PSM, ACS133, DSD advice).
### Glossary

<table>
<thead>
<tr>
<th>Agency</th>
<th>An Australian government entity.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGIFT</td>
<td>Australian Governments’ Interactive Functions Thesaurus (AGIFT), for functional description of records, information resources and services.</td>
</tr>
<tr>
<td>AGLS</td>
<td>Australian Government Locator Service (AGLS) is the Australian Government metadata standard. The AGLS metadata standard was developed to promote consistency of discovery of government resources. AGLS metadata, which is usually invisible to the end user, can be stored in HTML 'metatags', in XML, or in a metadata repository or directory that can be interrogated or harvested by external search engines. AGLS is now an official standard. AS 5044, AGLS Metadata Element Set, is the product of collaboration between the National Archives and Standards Australia. Based on an Australian Government standard, AS 5044 AGLS will enable web resources to be described consistently across all government, private and community sectors.</td>
</tr>
<tr>
<td>ASCII</td>
<td>American Standard Code for Information Interchange (ASCII) is the most common format for text files in computers and on the Internet. In an ASCII file, each alphabetic, numeric, or special character is represented with a 7-bit binary number (a string of seven 0s or 1s). 128 possible characters are defined.</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System (DNS), allows naming and location of Internet sites.</td>
</tr>
<tr>
<td>ebXML</td>
<td>e-business XML (ebXML) is a joint project of the UN and OASIS to develop an XML standard for business-to-business trade.</td>
</tr>
<tr>
<td>Fedlink</td>
<td>Fedlink is a Virtual Private Network that provides secure and trusted communications across the Internet.</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol (FTP), allows transfer of files between computers over the Internet. FTP is an application protocol.</td>
</tr>
<tr>
<td>GML</td>
<td>Geography Markup Language (GML), based on XML.</td>
</tr>
<tr>
<td>Guideline</td>
<td>A statement of desired, good or best practice.</td>
</tr>
<tr>
<td>HTML</td>
<td>Hypertext Markup Language (HTML) is the set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files on the World Wide Web. HTTP is an application protocol.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL (HTTPS) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is the use of Netscape’s Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.</td>
</tr>
</tbody>
</table>
IETF  Internet Engineering Task Force (IETF) coordinates the specification development process and maintains the agreed technical specifications for the evolution of the Internet architecture and the smooth operation of the Internet.

Integrated service delivery  Integrated service delivery (ISD) is the provision of government services (information and transactions) in a customer-oriented manner.

Customers have some choice of delivery channel and services from different agencies or jurisdictions are bundled into relevant groups for the convenience of customers. The customer’s service experience across channels is consistent, and customer contact history is available to all channels. Services involving transactions may require interaction with databases in multiple agencies.

Interoperability  Interoperability is the ability to transfer and use information in a uniform and efficient manner across multiple organisations and information technology systems. It underpins the level of benefits accruing to enterprises, government and the wider economy through e-commerce.

Metadata  Metadata is structured information that describes and allows us to find, manage, control and understand other information. In a web environment metadata acts like a virtual library catalogue - it helps government search engines to accurately and efficiently identify and retrieve web-based resources in response to search requests. To ensure that metadata is as useful as possible, it is important that it is applied consistently by agencies across the Australian Government.

Recognised resource discovery metadata schemes that are in active use by government in Australia include AGALS and its extensions and ANZLIC (geospatial).

MIME  Multi-Purpose Internet Mail Extensions (MIME) is an extension of the original Internet e-mail protocol that lets people use the protocol to exchange different kinds of data files on the Internet: audio, video, images, application programs, and other kinds, as well as the ASCII text handled in the original protocol, the Simple Mail Transport Protocol (SMTP).

NNTP  Network News Transfer Protocol (NNTP) is the protocol for managing notes posted on Usenet newsgroups.

Online service  Online services are services delivered via the Internet. An online service can be simple, such as provision of information, or more complex such as determining entitlement to and applying for a benefit online.

Open standards  Open Standards are recognised national or international platform independent standards. They are developed collaboratively through due process, are vendor neutral, do not rely on commercial intellectual property.

PKI  A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.
| **Protocol** | Protocol is used to mean agreed ways of working together, that is a common understanding of business rules required to operate a service or exchange data. It also has a specific meaning in IT circles of the special set of rules that end points in a telecommunication connection use when they communicate. Both end points must recognise and observe a protocol. Communications protocols are usually described in an industry or international standard. |
| **RDF** | The Resource Description Framework (RDF) is a general framework for semantic description of any Internet resource such as a Web site and its content. |
| **SMTP** | Simple Mail Transfer Protocol (SMTP) is a TCP/IP protocol used in sending and receiving e-mail. |
| **SOAP/XMLP** | Simple Object Access Protocol (SOAP/XMLP) uses web protocols to exchange from one computer to another. SOAP/XMLP specifies how to encode an HTTP header and an XML file so that one computer program can call a program in another computer and pass it information. It also specifies how to return a response. SOAP is a way for a program running in one kind of operating system (such as Windows 2000) to communicate with a program in the same or another kind of an operating system (such as Linux) by using the World Wide Web's Hypertext Transfer Protocol (HTTP) and its Extensible Markup Language (XML) as the mechanisms for information exchange. Since Web protocols are installed and available for use by all major operating system platforms, HTTP and XML provide an already at-hand solution to the problem of how programs running under different operating systems in a network can communicate with each other. SOAP specifies exactly how to encode an HTTP header and an XML file so that a program in one computer can call a program in another computer and pass it information. It also specifies how the called program can return a response. |
| **SSL** | Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. |
| **Standard** | Standard encompasses standards endorsed by a recognised standards setting authority; enacted in legislation; voluntary standards and agreed protocols. |
| **Structured Data** | Information that has been organised to allow identification and separation of the context of the information from its content. |
| **TAGS** | The Thesaurus of Australian Government Subjects (TAGS) describes Australian Government information and services from a subject or topic perspective. |
| **TCP/IP** | Transmission Control Protocol/Internet Protocol (TCP/IP) is the basic communication protocol of the Internet. It can also be used as a communications protocol in a private network. |
**TLS**

Transport Layer Security (TLS) is a security protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may interfere with or read any message. TLS is the successor to SSL.

**UDDI**

Universal Description, Discovery and Integration (UDDI) provides directory services to discover Internet-based business resources within the “web services” model.

**UDP**

User Datagram Protocol (UDP) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to TCP and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another.

**UML™**

Unified Modeling Language (UML™) is a standard notation for the modeling of real-world objects as a first step in developing an object-oriented design methodology.

**VPN**

A virtual private network (VPN) is a method of using a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization’s network.

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and other protocols. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a ‘channel’ that cannot be ‘entered’ by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

**W3C**

World Wide Web Consortium, the governing body for web standards. (http://www.w3.org/)

**Web services**

Web services are simple, self contained applications which perform functions, from simple requests to complicated business processes. The “web services” model uses WSDL, UDDI and SOAP/XMLP. A WSDL description is retrieved from the UDDI directory. WSDL descriptions allow the software systems of one business to extend to use those of the other directly. The services are invoked over the World Wide Web using the SOAP/XMLP protocol. Each of the components are XML based.

Where two agencies know about each other's web services they can link their SOAP/XMLP interfaces – provided all security concerns are managed appropriately. It is only where services are going to have unknown users that they need to be formally described by a language such as WSDL and entered into a directory such as UDDI.

**WSDL**

Web Services Definition Language (WSDL) describes how to use the software service interfaces of a registered business over the Internet within the “web services” model.
XML

Extensible Markup Language (XML) is a flexible way to create common information formats and share both the format and the data on the World Wide Web, Intranets, and elsewhere.

XML Schema

XML schema definition language for defining the structure, contents and semantics of XML documents.

XMLP

XML Protocol (XMLP), formally known as SOAP, uses web protocols to exchange from one computer to another. SOAP/XMLP specifies how to encode an HTTP header and an XML file so that one computer program can call a program in another computer and pass it information. It also specifies how to return a response.

XSL

Extensible Stylesheet Language (XSL) is the language for defining how a browser will display XML content to the user.