Australian Government
Technical Interoperability Framework

Contents

Foreword

More and more government operations and service delivery are spanning traditional agency boundaries, and this trend is likely to continue. Government agencies must be able to work together, share information and business processes to provide services which are tightly integrated across those agencies.

An important step to achieve seamless delivery of services across government is making sure that the tools we use to do business are compatible. Information and communications technology (ICT) is now the tool underpinning most government operations. This requires a whole-of-government ICT approach – a framework defining common standards and enablers.

Interoperability, or enabling seamless connections, is fundamental to reducing the cost of government and improving service outcomes to citizens. The technical interoperability framework provides this foundation of common standards to support collaboration across government agencies, the community and business sectors.

This latest version of the *Australian Government Technical Interoperability Framework (the Framework)* was developed by the Interoperability Framework Working Group (IFWG), a reference group of senior technical architects nominated by the Chief Information Officers' Committee (CIOC). The Australian Government Information Management Office (AGIMO) supported the review. This new version responds to developments in the ICT industry which are supporting business and government to be more interconnected. The Distributed Systems Technology Centre (DSTC) provided independent, expert advice during the course of the review.

The Framework specifies a conceptual model and agreed technical standards that support collaboration between Australian Government agencies. Adopting common technical protocols and standards will ensure government ICT systems interoperate in a trusted way with partners from industry and other governments. Interoperability will improve efficiency, reduce costs to business and government and will support agencies' capacity to respond to public policy developments.

The Framework's scope relates only to Australian Government agency interoperability. It does not affect the technologies deployed within an agency or constrain an agency's interactions outside the Australian Government.

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. It recognises that interoperability will develop out of independent, 'siloed' systems, but with a common business need – to exchange data. It is an important step towards multi-agency or whole-of-government service delivery.

This version of the Framework extends the range of standards in use by agencies and includes guidance on the nature of each standard and whether it is emerging or fading in its utility. The Framework is a living document and will develop as improvements and changes in technical, business and administrative processes emerge.

Ann Steward
Chair, Chief Information Officer Committee
July 2005

AGTIF is available electronically at:
http://www.agimo.gov.au/publications/2005/04/agtifv2#Australian20Technical20Framework.

Acknowledgements

The Chief Information Officer Committee (CIOC) required that Version 1 of the *Australian Government Technical Interoperability Framework* (AGTIF) be reviewed annually, and appointed the Interoperability Framework Working Group (IFWG) to undertake this task. The Australian Government Information Management Office (AGIMO) facilitated the review and provided secretariat services to the working group.

The IFWG provided technical advice and direction to develop the Framework.

The IFWG endorsed the following mission statement informing the activities of the Group:

> We believe that interoperability between agencies for the exchange of data and services is an important cornerstone for improving government business operations. This second version of the Australian Government Technical Interoperability Framework represents a collaborative effort by representatives of a number of agencies.
>
> This version of the Framework continues to support agencies to interoperate to deliver the government's policy outcomes, improve service delivery and reduce the cost of government.
>
> We commend Version 2 of the Australian Government Technical Interoperability Framework to you.

Members of the Interoperability Framework Working Group

- Tony Ablong, Manager, Information Support and Services Group, Department for Veterans' Affairs
- Jed Bartlett, Office of the Chief Information Officer, Department of Defence
- Don Bartley, Director, Technology Research Branch, Australian Bureau of Statistics
- John Busby, General Manager, Office of Spatial Data Management
- Jeremy Coleman, Technical Team Leader, Applications Development Support Section, Department of Education, Science and Training
- Steve Crisp, National Manager, Applications Architecture, Centrelink
- Todd Heather, Chief Technology Officer, Australian Taxation Office
- Kevin Fiebig, Director, Strategy and Coordination, Department of Family and Community Services
- Michael Glasson, Manager, IT Security, Department of Employment and Workplace Relations
- Angelo Paloni, Manager, Enterprise Architecture and Framework, Health Insurance Commission
- Thomas Schild, Business Systems Architect, Business Solutions Group, Department of Immigration and Multicultural and Indigenous Affairs
- Michael Tuite, Director, Business Systems, National Archives of Australia
- John Lalor, Service Improvement, Service Delivery Branch, Australian Government Information Management Office

1. What is the Technical Interoperability Framework? 1a

This Framework sets out a common language, conceptual model and standards that Australian Government agencies can employ as a basis for interoperating to deliver the Australian Government's policy and program priorities. This Framework does not impose obligations or in any way constrain agencies' abilities to undertake their core business.

Interoperability is defined as:

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

The Information Management Strategy Committee (IMSC) has endorsed an approach which divides interoperability into three domains:

- technical
- information
- business processes.

This document, the *Australian Government Technical Interoperability Framework* addresses the 'technical' domain. Technical interoperability supports information and business process interoperability.

The 'information interoperability' domain will provide a common methodology, definition and structure of information, along with shared services for its retrieval. The Information Interoperability Working Group is currently developing this agenda.

'Business process interoperability' will deal with common methods, processes and shared services for collaboration, including workflow, decision-making and business transactions.

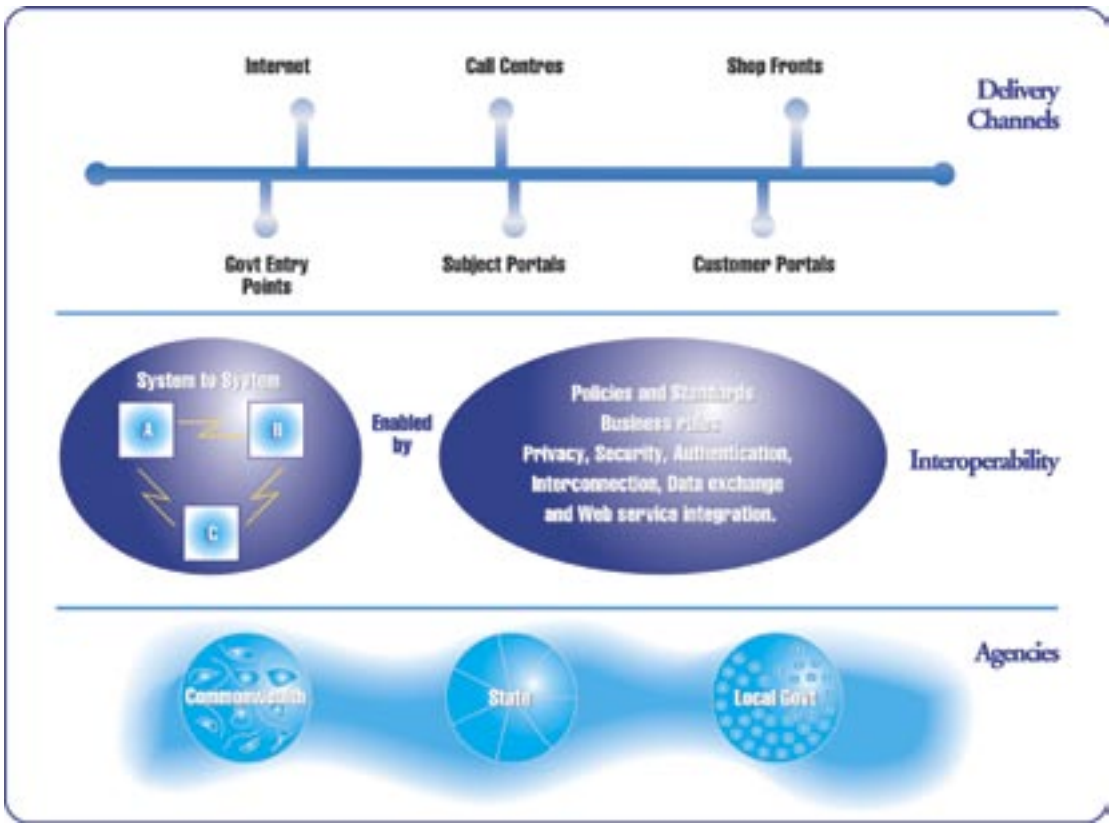
This Framework was developed to be consistent with broader industry trends. A successful Framework requires the involvement of all government Chief Information Officers. This means a strong commitment to collaboration, and to creating a cultural network that operates beyond internal systems. Crucially, this Framework will only be effective if agencies and departments support it and use it.

Ultimately, collaboration between agencies to deliver more efficient and effective government will require compatibility of the policy, legal and business environments across agencies. The Framework provides the first step in establishing this compatibility at the technical level for the exchange of data and harmonisation of business transactions within a trusted environment. This second version of the Framework extends Version 1 and now delivers a more comprehensive set of standards, while continuing to be a living, breathing framework that will grow over time.

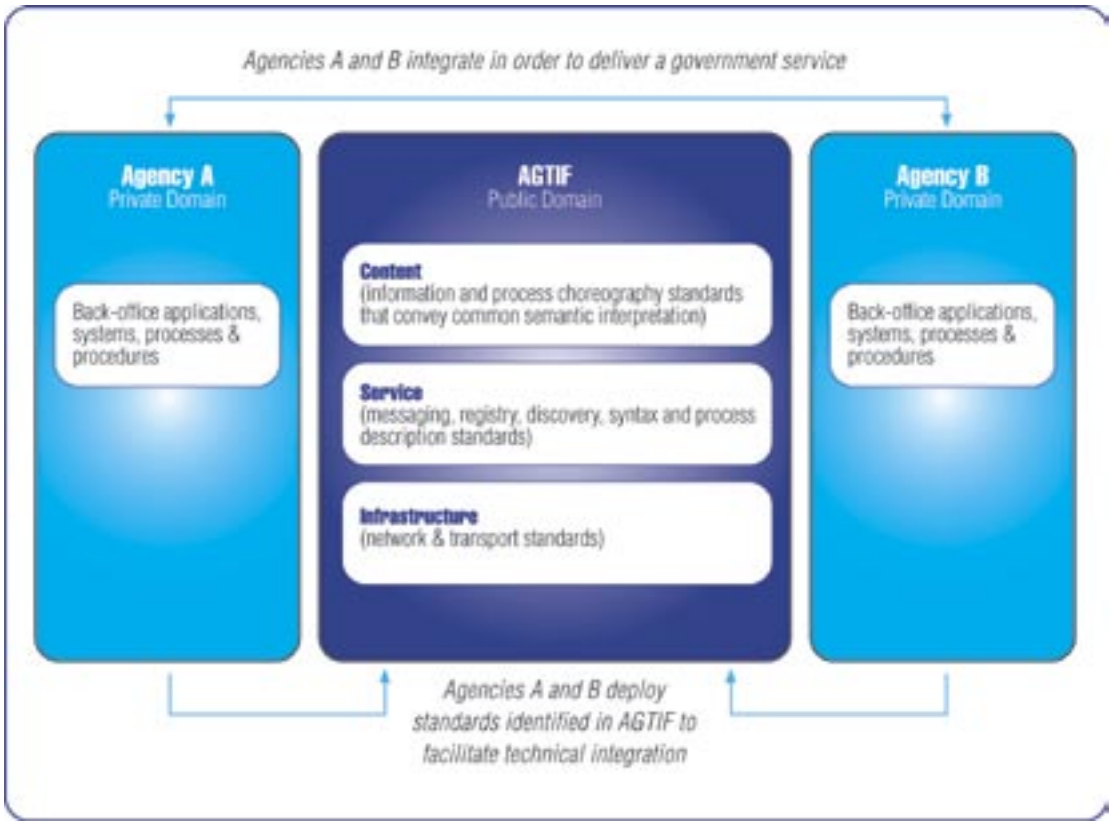
NB: Due to the fluid nature of technical standards, some standards listed in this document may also address issues related to content. These have been included pending development of other frameworks by the CIOC.

Figure 1 describes the business context within which interoperability is a key factor. As figure 1 shows, interoperability facilitates collaboration between government agencies and will, in the future, support collaborative service delivery and information sharing between all Australian jurisdictions.

Figure 1: Business Context



Interoperability thus supports improved service delivery to citizens; reducing the cost to government of delivering services and sharing information; and delivering greater economic efficiencies for the wider economy.



2.1 Principles

The following principles, endorsed by the Management Advisory Committee (MAC) underpin 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 as outlined in section 3.1.
- Trust and security are aspects of the Framework.
- The Framework will adapt to changing requirements over time and will be maintained at a strategic level.
- 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.

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 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 can:

- Raise awareness of the Framework within the agency.
- Adopt the Framework as a guide to agency policy.
- Ensure the Framework is used appropriately, for example, as business systems are ready for replacement consider the relevance of interoperability.
- 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 level of authentication are 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.
- 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.

2.3 Role of Australian Government Information Management Office (AGIMO)

This Framework has been developed in close consultation with key Australian Government agencies. The CIOC set the strategic direction through consultation and their endorsement of the Framework is collectively owned by CIOs. AGIMO will act as the focal point for managing and updating the Framework.

AGIMO's involvement in forums such as the World Wide Web Consortium (W3C) and the OASIS E-Government Asia-Pacific Technical Sub-Committee allows AGIMO to ensure consistency with global industry standards in the development of interoperability standards and policies.

AGIMO trialed the XML Clearinghouse in 2003. This was a proof of concept implementation of registry/repository technology. The purpose of the trial was to gain an understanding of how this technology could improve the management of cross-agency and cross-jurisdictional business processes, and to gain insight into the technical and governance requirements needed to successfully operate such a solution.

Based on the outcomes of the proof of concept, the intent is to migrate XML Clearinghouse to a pilot production version called GovDex. The aim is to position Govdex as a shared piece of collaborative infrastructure which agencies can leverage to rationalise the cost of integration and to transform service delivery.

3.1 Scope

Interoperability is about operating in a heterogeneous environment in which policy priorities, business strategies, administrative procedures, information requirements and technology systems differ between agencies.

This means interoperability is about addressing multiple domains. Figure 3 outlines three broadly defined domains.

Figure 3. Interoperability domains (endorsed by the IMSC in February 2004)

Business process domain	This domain comprises the commercial, legal, organisational and policy elements that facilitate interactions between agencies.
Information domain	This domain comprises elements that agencies use to align business processes and document payloads, and therefore generate common content interpretations. Elements include reference taxonomies and processes, code lists, data dictionaries and industry specific libraries. A Working Group has been established to progress this agenda.
Technical domain (This domain is the focus of this Framework)	This domain comprises elements used to deliver content across a community of interest. Elements include transport protocols, messaging standards, security standards, registry and discovery standards, syntax libraries, and service and process description languages.

While this Framework recognises the interdependence of these domains, its scope is limited to the technical domain.

The Framework does not seek to address the standards, policies and procedures that affect the information and business process domains. This is due to the context-specific nature of these domains in which agencies operate in different policy portfolios, engage different sets of stakeholders, and often have different information and business requirements.

AGIMO is currently working with stakeholders to coordinate a number of initiatives that are addressing issues within the information and business process domains.

The Framework only applies to the Australian Government jurisdiction. The Integrated Transaction Reference Group of the Online Council is considering a proposal to establish a national government interoperability framework, which aims to aggregate and harmonise Commonwealth, State and Local Government technical interoperability frameworks.

3.2 Conceptual Model

The Framework divides the technical domain into a series of groups.

The intent is not to prescribe an architecture but to provide a way to categorise a wide number of standards and to recognise linkages to the network and service layers. The groups are represented diagrammatically in Figure 2.

Figure 4. Technical domain - standards groups

<table>
<tr><td>Interconnection</td><td rowspan="6">Security</td></tr>
<tr><td>Data exchange</td></tr>
<tr><td>Discovery</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Metadata for Process and Data Description</td></tr>
<tr><td>Naming</td></tr>
</table>

To support agencies in applying this Framework a number of case studies have been provided. These will be updated over time and eventually supplemented by a 'how-to' guide.

Security

The Security category covers standards and technologies whose primary role is for supporting secure interoperation. Included in this category are standards and technologies for the encryption of data, public key infrastructure standards supporting the use of public and private encryption and decryption keys, digital signatures, and secure transmission protocols such as IPSEC.

Interconnection

The Interconnection category covers standards and technologies for connecting systems. Included within this category are basic connection protocols such as HTTP and FTP; the Web Services message exchange protocol SOAP and the service description language WSDL. Alternative distributed computing middleware such as J2EE (including Java RMI) or CORBA would also be located here. Asynchronous messaging standards such as JMS would be considered interconnection standards.

Data Exchange

The Data Exchange category contains standards and technologies for the description of the structure and encoding of data for exchange. These include protocols such as the email protocols SMTP and X.400, resource syndication protocols like RSS, as well as data markup languages such as XML and SGML. Basic character-set encodings would also be positioned here.

Discovery

The Discovery category covers standards and technologies for supporting the discovery and location of resources. These include metadata standards and thesaurus standards for supporting consistent description of resources. Also included are directory standards such as LDAP and X.500.

Presentation

The Presentation category covers standards related to the presentation of information. These standards allow data to be interpreted and presented in consistent ways when shared between systems. Such presentation standards include HTML (and XHTML) as well as selections from the wide range of image and streaming media formats. Also included would be the document encoding format RTF and a range of specialized markup languages, including markup for mobile devices.

Metadata for Process and Data Description

These standards are concerned with the sequencing of operations and their execution dependencies. Common amongst these standards are a range of workflow definition and description languages and the emerging Web Services coordination and choreography languages such as BPEL4WS.

The standards under this heading also support the description of the meaning of data elements, data structures and the interrelationships between data elements. Included within this fairly broad range of modelling standards are the UML, ER Diagrams, and flowcharts. Also covered would be XML Schema supporting the definition of XML instances.

Naming

The naming category covers the basic primitives for defining consistent names for resources. Standards in this category could perhaps be included within the data exchange category; however, given the importance of consistent naming schemes, it is worth distinguishing as a separate category.

In practice, there is often no neat and clean separation or categorization of standards. A given standard may belong in more than one category depending on the context or application. In this document, we attempt to position standards within the category that is most applicable and include cross-references from other categories where appropriate.

3.3 Presentation Guide

The Framework presents each standard against the following information.

Name & Version: The common name and most recent version under use for a given standard or technology.

Rights Model: Values in this column are: "Open" for freely available standards; "Proprietary" for standards whose use is controlled by a commercial organization; "Commercial" for standards that require payment for use; and "Government" indicating the item is a public sector resource.

Overview: A brief definition or description of the given item.

Custodian: The agency responsible for the item.

Usage: The current usage of this item. Either Fading; Current; or Emerging indicating the status of the item within a usage lifecycle. Fading refers to standards and technologies that, while still used, are receiving less support or are being superseded. Emerging refers to standards that do not currently have widespread use, but which are expected to receive more usage in future. Current refers to standards that have strong and ongoing support at this point in time.

Reference: A URL referring to definitive information relating to the item.

Comment: Any further comments that may be pertinent to the item or its use.

3.4 Standards Selection Criteria

The standards in the Framework are either currently used by, or are under consideration for use by, Australian Government agencies.

There are different types of standards that aid interoperability. Those that are an enabler for the description of content used by a "community of interest" are different in nature to the standard that is the content described. For example, the ISO 11179 Metadata Registry standards are used to create a registry of standard concepts and data items for the Health community within the AIHW Health Knowledgebase, similarly an Environmental Protection Authority might create a registry of Noxious Chemical Substances, and many others.

Clearly, interoperability activities will rely on the availability, status, reliability and common use of such information. The Framework focuses on the enabling standards. An ever increasing range of "content" standards is likely to emerge. Their use will depend upon the status they have in their "communities of interest". Over time, this will vary as the market forces relating to their acceptance and use play out.

The Framework catalogues both open and proprietary standards. Where feasible, preference is given to the deployment of open standards as these require no royalty payments, do not discriminate on the basis of implementation, allow extension, promote reusability, and reduce the risk of technical lock-in and high switching costs.

3.5 Policies for Data and Interconnection

This Framework draws on and incorporates previously established key policies for data definition and protection and for systems interconnection, as defined below:

For Security: *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://www.ag.gov.au/www/protectivesecurityHome.nsf/

The PSM refers to ACSI33:
Australian Communications-Electronic Security Instructions 33 (ACSI33) available at http://www.dsd.gov.au/library/infosec/acsi33.html maintained by the Defence Signals Directorate.

Between government agencies, where connection is over the Internet, the use of Fedlink (http://www.fedlink.gov.au/) encryption routers will ensure confidentiality.

For Authentication: The Australian Government e-Authentication Framework (AGAF) comprises a set of principles for e-authentication for the whole of government. It is based on four assurance levels that are matched to the risk associated with a transaction. Overview information and implementation guides can be found at http://www.agimo.gov.au/infrastructure/authentication/agaf.

For Privacy: Australian Government agencies are bound by a regulatory framework, administered by the Office of the Federal Privacy Commissioner. A paper issued by the Office (Privacy in Australia – August 2002) (http://www.privacy.gov.au/publications/pia1.html) has an overview of privacy regulation in Australia, and covers some of the important privacy issues in Australia.

For Procurement: Australian Government agencies should refer to the guide Government Framework for National Cooperation on Electronic Procurement June 2002, by the Australian Procurement and Construction Council http://www.apcc.gov.au/docs/APCCFRAMEWORK2002.pdf

For Data definition: Policy is to use existing standards - where formal Australian standards exist (such as AS 4590 - the Australian standard for interchange of client information, or the *Australian Government Locator Service* http://www.naa.gov.au/recordkeeping/gov_online/agls/cim/cim_manual.html for Commonwealth use of metadata) they should be used, or if considered not exactly suitable, then steps taken to update the standard.

For Government Domain Naming: The policy is set by the Online Council and managed by Australian Government Information Management Office (AGIMO) http://www.domainname.gov.au/register.html

3.6 Standards Catalogue

3.6.1 Security

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
1	ACSI33 June 2004 or later release.	Australian Government Information Technology Security Manual (Australian Communications-Electronic Security Instructions 33)	Defence Signals Directorate.	Current	http://www.dsd.gov.au/library/infosec/acsi33.html	Multiple releases per year. SECURITY-IN-CONFIDENCE and UNCLASSIFIED versions.
2	S/MIME ESS Version 3	Secure/Multipurpose Internet Mail Extensions with Encrypted Security Service. A standard that extends the MIME specifications to support the signing and encryption of e-mail transmitted across the Internet.	IETF	Current	http://www.faqs.org/rfcs/rfc2632.html http://www.faqs.org/rfcs/rfc2633.html	RFC 2633 June 1999, message specification. RFC 2632 June 1999, certificate handling.
3	SAML v1.1	Security Assertions Markup Language (SAML) is an XML-based framework for Web services that enables the exchange of authentication and authorization information	OASIS	Current / Emerging	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security	SAML 1.0 November 2002 SAML 1.1 August 2003 SAML 2.0 underway to deliver federated security
4	SSL version 3	Secure Socket Layer. A protocol used for secure Internet communications. See ACSI 33 for guidance.	Netscape	Current	http://wp.netscape.com/eng/ssl3/	Developed by Netspace in 1996, basis for TLS in 1999.
5	TLS	Transport Layer Security. See ACSI 33 for guidance. TLS (RFC 2246:1999 updated by RFC 3546:2003)	IETF	Current	http://www.ietf.org/rfc/rfc2246.txt http://www.ietf.org/rfc/rfc3546.txt	Last TLS update June 2003, TLS Protocol Compression Methods RFC 3749 May 2004 TLS is an enhancement of SSL version 3
6	WS - Security	Ensures security of messages transmitted between web services components.	OASIS	Current	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss	WS-I Basic Security Profile Version 1.0 is preferred over this but only emerging at this stage
7	WS-I - Basic Security Profile Version 1.0	Web Services-Interoperability Organization Web Services - Basic Security Profile Version 1.0	Web Services-Interoperability Organization (WS-I)	Emerging	http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html	Still evolving – latest working draft May 2004
8	X.509	International standard for identity certificates.	ITU-T	Current	http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-X.509-200003-I	Part of hierarchical X.500 specification. IEEE RFC 2459. Approved March 2000.

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
9	XML-DSIG	An XML compliant syntax used for representing the signature of Web resources and procedures for computing and verifying such signatures.	Joint IETF / W3C	Emerging	http://www.w3.org/Signature/	Syntax and Processing – Feb 2002 XPath Filter 2.0 – Nov 2002 Canonical XML 1.0 – March 2001

3.6.2 Discovery

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
1	AGLS version 1.3	Australian Government Locator Service - an Australian metadata standard (AS5044) for supporting consistent discovery of a range of information resources held by government agencies.	National Archives of Australia / Standards Australia	Current	http://www.naa.gov.au/recordkeeping/gov_online/agls/summary.html	AGLS is based on the Dublin Core metadata element set. Published Dec 2002. National Archives coordinates maintenance function.
2	Domain Name Service (DNS)	The Domain Name System (or Service) is a service for mapping between domain names and corresponding IP addresses.	IETF	Current	http://www.ietf.org/rfc/rfc1035.txt IETF STD 13:1987, RFC 1034:1987 and RFC 1035:1987 updated by RFCs 1101:1989 through 3658:2003	Used for Government Domain Naming
3	Dublin Core Standard	A simple and extensible metadata element set intended to facilitate discovery of electronic resources.	DCMI	Current	http://www.dublincore.org/	The Dublin Core metadata element set is the basis for the AGLS metadata standard.
4	ISO1911:2003	Defines the schema required for describing geographic information and services – the extent, the quality, the spatial and temporal schema, spatial reference, and distribution of digital geographic data.	ISO	Current	http://www.iso.ch/	An Australian Government profile is under development (contact ODSM for more information)
5	LDAP version 3	Lightweight Directory Access Protocol, a standard mechanism for accessing directory services	IETF	Current	http://www.ietf.org/rfc/rfc2251.txt	Stable
6	METS	Metadata Object Description Standard – Structure for encoding descriptive, administrative, and structural metadata for objects in a digital library.	Library of Congress	Current	http://www.loc.gov/standards	Current MTS XML Schema version 1.3 May 2003

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
7	MIX	NISO Metadata for Images in XML – XML schema for encoding technical elements required to manage digital image collections	Library of Congress	Current/ Emerging	http://www.loc.gov/standards	Current Version 0.2, April 6, 2004
8	OAI Harvesting protocol version 2	Open Archives Initiative - supports access to web-accessible material through interoperable repositories for metadata sharing, publishing and archiving	OAI	Emerging	http://www.openarchives.org/index.html	Harvesting protocol version 2 2003.
9	ODRL	Open Digital Rights Language	IPR Systems	Current	http://www.odrl.net/	Version 1.1 Sept 2002 is a W3C note.
10	RDF	Resource Description Framework – A method for specifying the syntax of metadata, used to exchange metadata.	W3C	Current	http://www.w3.org/rdf	Used as a lightweight ontology system to support the exchange of knowledge on the web.
11	Recordkeeping Metadata Standard for Common-wealth Agencies	Describes the metadata that should be captured by Recordkeeping Systems.	National Archives of Australia	Current	http://www.naa.gov.au/	The Recordkeeping Metadata Standard for Commonwealth Agencies (1999) includes references to Australian Standard AS 4390 – 1996, Records Management. This Standard has now been superseded by the Australian Standard for Records Management AS ISO 15489 – 2002 which is based significantly on AS 4390.
12	UDDI version 2	Universal Description, Discovery and Integration protocol - A directory model for web services. Part of WS-I Basic Profile 1.1	OASIS	Current	http://www.uddi.org/specification.html	Version 3.01 has been approved as a standard in October 2003.
13	WSDL version 1.1	Web Services Description Language - an XML-based language used to describe Web services.	W3C	Current	http://www.w3.org/2002/ws/desc/	Part of WS-I Basic Profile 1.1
14	XrML	EXtensible Rights Markup Language	ContentGuard	Current	http://www.xrml.org/	Version 2.0 2001

3.6.3 Interconnection

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
1	BGP4	Border Gateway Protocol - For internetworking between WAN	IETF	Current	http://www.ietf.org/rfc/rfc1771.txt	Version 4
2	Fedlink	A Virtual Private Network (VPN) that allows Commonwealth departments and agencies to transmit and receive information securely to PROTECTED level using the Internet.	Australian Government	Current	http://www.fedlink.gov.au/	Cabinet level direction has been given to all Agencies to use Fedlink.
3	FTP	File Transfer Protocol: The standard Internet protocol for transferring files from one computer to another.	IETF	Current	http://www.ietf.org/rfc/rfc765.txt	FTP and IBM formats
4	HTTP v1.1	HyperText Transfer Protocol, the underlying protocol used by the World Wide Web for the transmission of hypertext files.	IETF	Current	http://www.ietf.org/rfc/rfc2616.txt	June 1999
5	HTTPS	A secure version of HTTP, implemented using the secure sockets layer, TLS.	IETF	Current	http://www.ietf.org/rfc/rfc2818.txt	May 2000
6	Multiprotocol Extensions for BGP-4 and Extensions for IPv6 Inter-Domain Routing	For internetworking between WAN	IETF	Emerging	Multiprotocol Extensions for BGP-4: http://www.ietf.org/rfc/rfc2858.txt Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing: http://www.ietf.org/rfc/rfc2545.txt	
7	SOAP version 1.1	Simple Object Access Protocol - A lightweight, XML-based messaging protocol that is the encoding standard for web services messages.	W3C	Current	http://www.w3.org/TR/soap/	W3C Recommendation 24 June 2003. Part of WS-I Basic Profile 1.1
8	SOAP version 1.2	see SOAP version 1.1	W3C	Emerging	http://www.w3.org/TR/soap/	
9	TCP/IP version 4	Transmission Control Protocol/ Internet Protocol, the basic communication protocol that is the foundation of the Internet.	IETF	Current	TCP: http://www.ietf.org/rfc/rfc793.txt IPv4: (RFC 791, 792, 919, 922, 1112)	September 1981
10	WSDL	See Section 3.8.2 Discovery				

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
11	WS-I Basic Profile 1.1	Web Services Interoperability Profile - a set of non-proprietary Web services specifications, along with clarifications and amendments to those specifications that promote interoperability.	WS-I	Current	http://www.ws-i.org/	August 2004
12	WS-I Simple SOAP Binding Profile 1.0	The Profile defines the use of XML envelopes for transmitting messages and places certain constraints on their use.	WS-I	Current	http://www.ws-i.org/	August 2004
13	WS-I Attachments Profile 1.0	Defines a MIME multipart/ related structure for packaging attachments with SOAP messages.	WS-I	Current	http://www.ws-i.org/	August 2004

3.6.4 Data Exchange

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
1	AGIFT	Australian Government Interactive Functions Thesaurus	National Archives of Australia	Current	http://www.naa.gov.au/recordkeeping/gov_online/agift/summary.html	The DIRKS Manual Appendix 6 – Practical advice for using Keyword AAA and AGIFT terms provides advice on using AGIFT terms in classification tools.
2	ANSI HL7 Health Level Seven Standard Version 2.4 - Application Protocol for Electronic Data Interchange in Healthcare Environments.	Health Level 7. A set of healthcare specific standards for data exchange between computer applications.	ANSI	Current	http://www.hl7.org/	Health Level Seven Standard Version 2.4 October 6, 2000.
3	ANZIC	Australian and New Zealand industrial classification codes.	Australian Bureau of Statistics	Current	http://www.abs.gov.au/ausstats/abs@.nsf/0/7cd8aebba7225c4eca25697e0018faf3?OpenDocument&Highlight=0,anzsic	ABS Standards
4	AS4590 - 1999	Australian standard for interchange of client data	Standards Australia	Current	http://www.standards.com.au/	

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
5	ebXML Standard Message Service Specification Version 2.0 (now ISO/TS 1500 series)	Adds security and reliability extensions to SOAP	OASIS / ISO	Current	http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf and http://www.iso.org/	ISO/TS 15000-1:2004 Electronic business eXtensible Markup Language (ebXML) - Part 1: Collaboration-protocol profile and agreement specification (ebCPP) Part 2: Message service specification (ebMS) Part 3: Registry information model specification (ebRIM) Part 4: Registry services specification (ebRS)
6	ISO 11179 Information Technology – Metadata Registries (MDR)	Framework for the specification and standardization of data/ metadata elements.	ISO	Current	http://www.iso.org/	Under use for standardising data element repositories, and work on Taxonomies, Thesaurus and Dictionary. Six Parts: 1: Framework; 2: Classification for administered items; 3: Registry metamodel and basic attributes; 4: Formulation of data definitions; 5: Naming and identification principles; 6: Registration
7	ISO15022 - XML Design rules	Supports the design of message types and their specific information flows.	ISO	Current	http://www.iso15022.org/	ISO 15022 supports EDIFACT.
8	MIME	Multipurpose Internet Mail Extensions. MIME is a standard for the embedding of binary data of known types (images, sound, video, and so on) into e-mail handled by ordinary Internet electronic mail interchange protocols.	IETF	Current	http://www.ietf.org/rfc/rfc1521.txt	September 1993
9	SMTP	Simple Mail Transfer Protocol – A protocol used to send e-mail on the Internet.	IETF	Current	http://www.ietf.org/rfc/rfc0821.txt	August 1982

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
10	TAGS	Thesaurus of Australian Government Subjects provides common terminology for describing Commonwealth information and services	AGIMO	Current	http://www.agimo.gov.au/services/tags	Version 1 January 2002
11	UN/EDIFACT	Electronic Data Interchange for Administration, Commerce, and Transport. The United Nations EDI standard.	UN ECE	Current	http://www.unece.org/trade/untdid/welcome.htm	D0.4A May 2004
12	UNICODE	A 2-byte character set, developed as a universal character set for international use.		Current	http://www.unicode.org/	Current version 4.01 2003
13	XBRL Meta Model v2.1.1	eXtensible Business Reporting Language - an XML language for business reporting	XBRL	Current	http://www.xbrl.org/	Version 2.1 January 2004. Note: XBRL web site ONLY supports viewing with Microsoft Internet Explorer.
14	XMI	XML Metadata Interchange Format. An open information interchange model.	OMG	Current	http://www.omg.org/technology/documents/formal/xmi.htm	Version 2.0 May 2003
15	XML 1.0 (Third Edition)	eXtensible Markup Language - a metalanguage (a way to define tag sets) that supports design of customized markup languages.	W3C	Current	http://www.w3.org/XML/	W3C Recommendation February 2004
16	XSL version 1.0	eXtensible Stylesheet Language - A family of recommendations for describing stylesheets for XML document transformation and presentation.	W3C	Current	http://www.w3.org/Style/XSL/	Also known as XSL-FO
17	XSLT version 1.0	XSL Transformations - a language for transforming XML documents into other XML documents.	W3C	Current	http://www.w3.org/Style/XSL/	Increasing use, particularly in new apps

3.6.5 Presentation Encoding Formats

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
1	BWF	Broadcast Wave Format – a file and metadata format based on Microsoft's WAVE format for transferring files between digital audio workstations.	European Broadcast Union	Current	http://www.ebu.ch/	EBU Technical Recommendation R97 1999
2	GIF	Graphic Interchange Format - A common format for image files.	CompuServe	Current	http://www.w3.org/Graphics/GIF/spec-gif89a.txt	Standard is owned by CompuServe, but available under non-exclusive freely-available license. Most recent version: v89a
3	HTML version 4.01	HyperText Markup Language - the coding language used to create Hypertext documents for use on the World Wide Web.	W3C	Current	RFC 2854:2000 http://www.ietf.org/rfc/rfc2854.txt	June 2000
4	JPEG	Joint Photographic Experts Group - A common graphic image file format and image compression algorithm.	JPEG	Current	http://www.jpeg.org/jpeg/	JPEG is ISO/IEC IS 10918-1 | ITU-T Recommendation T.81
5	MPEG-1	Moving Picture Experts Group - Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s	Moving Picture Experts Group/ ISO	Current	http://www.chiariglione.org/mpeg/standards/mpeg-1/mpeg-1.htm	ISO/IEC 11172-1:1993 with most recent update 1999. MPEG-1 is the standard on which such products as Video CD and MP3 are based
6	MPEG-2	Generic coding of moving pictures and associated audio information	Moving Picture Experts Group/ ISO	Current	http://www.chiariglione.org/mpeg/standards/mpeg-2/mpeg-2.htm	MPEG-2 is in 9 parts. The first three parts of MPEG-2 have reached International Standard status in 2000 or earlier. Standard on which such products as Digital Television set top boxes and DVD are based
7	MPEG-4	MPEG-4 provides the standardized technological elements enabling the integration of the production, distribution and content access paradigms of the three fields.	Moving Picture Experts Group/ ISO	Current	http://www.chiariglione.org/mpeg/standards/mpeg-4/mpeg-4.htm	Standard for multimedia for the fixed and mobile web. MPEG-4 is: ISO/IEC 14496 1999
8	MPEG-7	"Multimedia Content Description Interface" - Standard for description and search of audio and visual content.	Moving Picture Experts Group/ ISO	Emerging	http://www.chiariglione.org/mpeg/standards/mpeg-7/mpeg-7.htm	International standard 2001

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
9	MPEG-21	"Multimedia Framework"	Moving Picture Experts Group/ ISO	Emerging	http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm	ISO/IEC 21000–N series still under standardization.
10	MXF	Material eXchange Format – an open file format for the interchange of audio-visual material with associated data and metadata.	Pro-MPEG Forum & SMPTE	Emerging	http://www.pro-mpeg.org/	March 2004
11	PDF (Adobe Specification 1.5)	Portable Document Format, a universal file format created by Adobe Systems allowing users to distribute, read, and view electronic documents with all formatting, fonts, text sizes, graphics, color, etc. intact.	Adobe Systems	Current	http://partners.adobe.com/asn/tech/pdf/specifications.jsp	PDF Reference, Fourth Edition, Version 1.5 August 2003. Proprietary standard
12	PNG	Portable Network Graphics – a format for storing bit-mapped images	W3C	Current	http://www.w3.org/TR/PNG/	
13	RTF encoded document	Rich Text Format - A method of encoding text formatting and document structure using the ASCII character set.	Microsoft	Current	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnrtfspec/html/rtfspec.asp	Proprietary standard
14	SVG version 1.1	Scalable Vector Graphics - XML-based graphics format	W3C	Current	http://www.w3.org/TR/SVG11/	W3C Recommendation 14 January 2003
15	TIFF version 6.0	Tagged Image File Format - A widely-supported tag-based bitmap image format	Adobe Systems	Current	http://www.adobe.com/	Proprietary standard
16	XHTML version 1.0:2002	Extensible Hypertext Markup Language - A reformulation of HTML 4.0 in XML 1.0	W3C	Current	http://www.w3.org/MarkUp/	W3C Recommendation 26 January 2000, revised 1 August 2002
17	XML 1.0 (Third Edition)	eXtensible Markup Language - a metalanguage (a way to define tag sets) that supports design of customized markup languages.	W3C	Current	http://www.w3.org/XML/	W3C Recommendation February 2004

3.6.6 Metadata for Process and Data Description

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
1.	BPEL4WS	Business Process Execution Language for Web Services - a language for the specification of business processes and business interaction protocols.	IBM, Microsoft et. al. industry consortium	Emerging	http://www-106.ibm.com/developerworks/library/ws-bpel/	Version 1.1 May 2003
2.	ER Diagrams	Entity-Relationship diagram - a diagramming notation used in data modeling for relational data bases.		Current	http://bit.csc.lsu.edu/~chen/pdf/erd.pdf	Still in use, particularly in older apps.
3.	ISO 11179 Information Technology – Metadata Registries (MDR) Part 4 Formulation of data definitions.	See Section 3.6.4 Standard 6				
4.	XML schema Parts 0-2:2001	An XML-based language for defining the structure of XML documents and for specifying datatypes for attribute values and element content.	W3C	Emerging	http://www.w3.org/XML/Schema	W3C Recommendation, 2 May 2001. XML Schema 1.1 under development.

3.6.7 Naming

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
1.	URI	Uniform Resource Identifier - the generic term for a coded string that identifies a (typically Internet) resource.	IETF	Current	http://www.ietf.org/rfc/rfc2396.txt	August 1998
2.	URL	Uniform Resource Locator - the global address of documents and other resources on the World Wide Web.	IETF	Current	http://www.ietf.org/rfc/rfc1738.txt	December 1994

Nr.	Name & Version	Overview	Custodian	Status	Reference	Comment
3.	Namespaces in XML, W3C Recommendation, 14 Jan 1999	W3C Recommendation	W3C	Current	RFC 2396 Uniform Resource Identifiers (URI): Generic Syntax: http://www.ietf.org/rfc/rfc2396.txt RFC 3406 Uniform Resource Names (URN) Namespace Definition Mechanisms: http://www.ietf.org/rfc/rfc3406.txt http://www.w3.org/TR/REC-xml-names/	
4.	ISO 3166 Code Lists	2-letter and 3-letter country code representation standard.	ISO	Current	http://www.iso.org/	2-letter country codes only are applicable for AGTIF interoperability
5.	ISO 8601, Data elements and interchange formats – Information interchange – Representation of dates and times	Date and time representation standard.	ISO	Current	http://www.iso.org/	
6.	ISO 11179 Information Technology – Metadata Registries (MDR) Part 5 Naming and identification principles.	See Section 3.6.4 Standard 6				

4.1 Case Study: ATO – DIMIA TFN Entitlement

4.1.1 Administrative Details

Case study title:	ATO-DIMIA TFN entitlement
Organisations involved:	ATO-DIMIA
Key contact information:	DIMIA - Thomas Schild (Business Systems Architect) ATO - Todd Heather (Chief Technology Officer), Craig Boscoe (Project Management)

4.1.2 Abstract of Case Study

The Individual TFN Auto-Registration application was developed primarily to further improve the integrity of the Tax File Number system. The first phase achieves this by only issuing a TFN to eligible persons (generally permanent migrants and those temporary visitors who have the right to work whilst visiting and who have arrived in Australia). Other business benefits for the ATO and the ATO's clients included:

- Reduced administrative burdens on both the ATO and the applicant by allowing for online self-service which removes the need for:
  - the applicant to attend an ATO Access site
  - the ATO to manually process the proof of identity process and then key the application.
- Improvements to the timeliness of the TFN issuing process.
- Inform permanent migrants and those temporary visitors with work rights of their rights and obligations regarding the Australian taxation system.
- Create an automated risk assessment engine to provide a determination of the risk for each TFN applicant with low risk applications automatically processed without manual intervention.

There have been benefits also to interoperability between the two Agencies, such as:

- Establishing a set of reusable components for further extension of the Auto-Registration processes.
- Facilitating improved data sharing between DIMIA and the ATO to improve compliance with legislation administered by both areas.

A key part of this process was for the ATO be able to successfully obtain from DIMIA information that enabled both the determination of eligibility and the completion of the risk assessment for each application. The key information requirements are to confirm a visitor's visa status (do they have the right to work or permanently reside in Australia), be informed of previous visits to Australia and to confirm their presence in Australia. To allow this DIMIA developed a number of visa status services that could be invoked by ATO systems. The various services communicate with one another asynchronously over a dedicated, secure link.

In addition to the technical aspects of the project, a memorandum of understanding was developed to govern operations.

Proposed Technical Solution

The proposed technical solution is one that has been jointly determined by the respective areas of the ATO and DIMIA. It has been developed in consultation with the relevant security, privacy and enterprise architecture teams.

4.1.3 List of Case Study Technologies and Standards

DIMIA Solution

All of the DIMIA services were developed using Natural and COBOL.

At the DIMIA end of the link i-Connect is used to process the XML and interface to MQSeries.

Shared Infrastructure

The government optical fibre network ICON was used as the communication carrier. Network protocol is TCP/IP. MQ Series from IBM is used as the transport middleware. ebXML message services specification is used to mange the conversations between the processes. Payloads conform to the ebXML specifications.

ATO Solution

At the ATO Microsoft Biztalk is used to process the XML.

Mapping Solution to Interoperability Framework

The following section maps the ATO- DIMIA interoperability functionality against the categories described in the AGTIF, and shown below.

Solution AGTIF Mapping

AGTIF Category	DIMIA	ATO	Shared	Comments/issues
Security			Secure interconnection is provided at the transport level. Participating processes are authorised by name and the link between the 2 agencies is encrypted. Access to ICON network is limited to Government Agencies only.	
Discovery	Not applicable	Not applicable.		
Interconnection			Communications protocol is implemented using a Virtual Private Network (VPN), ICON and the messaging middleware MQSeries. TCP/IP is used as the network protocol over the VPN.	
Data Exchange			SOAP with attachments, containing an ebXML message.	Mix of synchronous and asynchronous data exchange. Synchronous exchange is required to respond in less than 10 seconds. SOAP envelope provides standard structure of message. Message formats and standards agreed between DIMIA and ATO.
Presentation	Not applicable	Not applicable.		
Process modelling		ATO uses UML to model process interactions.		
Data modelling		UML Class modelling to model Object Classes and interfaces.		
Naming	Not applicable	Not applicable.		

4.1.4 System Architecture

The system is built as a set of loosely coupled processes. ATO components request information asynchronously from DIMIA services. The requests are packaged as ebXML documents. Replies are formulated as ebXML documents. The conversation between the processes conforms to the rules of the ebXML message specification.

4.1.5 Information Model

DIMIA visa status information is required to finalise a TFN allocation request for ATO clients. ATO requests include person identification information. DIMIA replies include the dispatched data plus any relevant visa status information that has been discovered.

4.1.6 Security and Rollout

The information passed is classified as personal in confidence and needs to be protected to that level. The required security is obtained using a secure pipes model. Participating processes are authorised by name to the security systems at each end. The link between the two agencies is encrypted. Access to the ICON network is limited to government agencies only.

4.1.7 Issues and Lessons Learned

Establishing the Link

This was a simple process at the technology level but time consuming, so there is a need to plan to initiate these activities early in such a project.

Developing the Interoperation

Considerable project effort was required to create the payloads and overcome ambiguities in the specifications related to the processing of the XML. DIMIA's services are mainframe based and some XML processing tools had to be created to facilitate this. At the ATO end Microsoft tools were used. The default XML processing in Microsoft tools included a number of details not mandated in the ebXML specification and workarounds had to be developed.

Agreeing on Semantics.

The ebXML message service specification helped to reduce the effort in defining the semantics of the message headers, payload and error messages.

Developing the Services

This was a straightforward area of the development.

Setting up the Memorandum of Understanding Governing Operations.

This required negotiation between the relevant business sponsors in the two Agencies

Technologies and Standards

None of the technologies used is leading edge. This was a conscious decision on the part of DIMIA and ATO. ICON was chosen as a low cost communications link. MQSeries was chosen for its robustness. It was recognised that standards should be applied at the data exchange layer. ebXML message services was chosen because it is a vendor independent specification covering document creation, error handling and high level protocols for routing and conversation management.

4.2 Case Study: HIC-ATO 2004 e-tax Customer Access Pilot

4.2.1 Administrative Details

Case study title: 2004 e-tax Customer Access Pilot

Organisations involved: HIC, ATO, AGIMO, Microsoft

Key contact information: HIC - Jeff Mitchell
HIC - Steve Nolan
ATO - Todd Heather (Chief Technology Officer),
ATO - John McAlister (Project Management)

4.2.2 Abstract of Case Study

The e-tax Customer Access pilot is an initiative being undertaken by the HIC and the ATO that will enable Medicare card holders to access their Medicare Financial Tax Statement data at the time they are completing their 2004 income tax return via e-tax. The pilot will run from July to October 2004, coinciding with the 2004 individual lodgement tax return period. The pilot was envisaged to target approximately 300 participants however consumer interest has resulted in requests for over 1000 registration packages, with in excess of 600 registrations received at early June. Following evaluation of the pilot, the HIC and the ATO are intending to provide this service to all e-tax users from 2005.

4.2.3 Background

Discussion between the HIC and the ATO senior executives in 2003 recognised that consistency of clients between the two agencies existed, and investigation was made into how the agencies could work together to improve the client experience, while supporting the Whole-of-Government initiative.

In November 2003 the ATO endorsed the Joint HIC and ATO Pilot to develop a capability to populate e-tax 2004, Net Medical Expenses, with data held by the HIC.

The HIC is establishing a Medicare interface to access medical expenses information through a Web Service, as well as providing an application to register participants in the pilot. The ATO is building an extension to the e-tax 2004 application to invoke the HIC service. A number of new e-tax screens have been developed which contain information for pilot participants on the steps involved in downloading their data from the HIC, and the correct use of this information when determining their entitlement to a claim.

The e-tax pilot will trial an easier capability for a client to complete the Net Medical Expenses item on their tax return by providing both an electronic record of the Financial Tax Statement and by populating the Net Medical Expenses worksheet within e-tax with the data held by the HIC. This removes the need to directly approach the HIC for a statement to be provided by mail.

A short-term electronic link has been installed between the HIC and the ATO to facilitate the transfer of the pilot data once initiated by the participant.

Microsoft Australia, through the Australian Government Information Management Office (AGIMO), is assisting to fund this project through the Strategic Partner Fund.

Piloting a solution required agreed principles and joint design effort.

The HIC and the ATO e-tax Customer Access pilot will provide Medicare card holders with their Financial Tax Statement information at the time they are completing their e-tax 2004 income tax return. The pilot will run in partnership between the HIC and the ATO from July to October 2004, coinciding with the 2004 individual tax return lodgement period.

Underlying business architecture principles have been agreed which will:

- Ensure secure end-to-end transmission of client information.
- Require a secure data link to be established between the ATO and the HIC.

Privacy and security of client data will be protected as the agreed ATO and HIC solution will:

- Not rely on the transfer of either a client's Medicare Card Number nor their Tax File Number between the ATO or the HIC.
- Not match client data between the ATO and the HIC.
- Not retain a client's HIC Financial Tax Statement data in any way on the ATO infrastructure..

Due to the sensitive nature of information to be transmitted over the external link, security and client verification is of major concern in establishing the trusted inter-agency communications environment. The key areas of consideration for the design included:

- Confidentiality and integrity of data over the link.
- Authentication/authorisation of clients by both the ATO and the HIC.
- System level authentication and access control between the HIC servers and the e-tax servers.
- Conformance to both the ATO and the HIC security architecture requirements and directions.
- Conformance to both the ATO and the HIC procedures for system development, acceptance testing, security penetration/vulnerability testing and system release.
- Ensuring secure administrative access (authentication of administrators and secure access channel) to the systems.
- Consideration of impact of availability of infrastructure in either Agency on the client.
- Integrated audit logging and monitoring capability covering both the ATO and the HIC end-to-end access activities.

Proposed Technical Solution

The proposed technical solution is one that has been jointly determined by the respective areas of the ATO and the HIC. It has been developed in consultation with the relevant security, privacy and enterprise architecture teams.

4.2.4 List of Case Study Technologies and Standards

HIC solution

The HIC receives around 100,000 requests for Medicare Financial Tax Statements each year, placing it within the top six HIC consumer online requests. Currently no fully online service is available through the HIC, therefore the statement is provided over the counter or via mail upon client request.

The HIC has built a consent database and application to manage allocation of consent to access Medicare details, and to manage issue of a Reference number to clients. The Reference number is the basis for authentication of the HIC services. The HIC has also provided a Web Service to access data in the legacy HIC Medicare application. The Technology details of these solution components are:

HIC Consent database and application

This is a new application to manage registrations for the pilot participation, validate rights to access Medicare details, and provide Reference numbers. The technologies used in this application include:

- Application platform is J2EE running on IBM WebSphere.
- Database is IBM DB2 running on AIX midrange servers, accessed by Java Classes using JDBC.
- A STRUTS based presentation layer, which implements an MVC-2 design pattern.
- JSP and Java programming languages.

HIC Medicare Application

This is a heritage mainframe application with a CICS/Cobol code base accessing data stored in DB2 and VSAM databases. The Medicare application is invoked by a mid-range Java-based tier via IIOP.

HIC e-tax Web Service

The e-tax Web Service validates the pilot participants' requests against the consent database, and requests statement details from the Medicare application. The Web Service is built on:

- Java programming language, hosted on Websphere/J2EE.
- Standard Web Service interconnection technologies SOAP and WSDL.
- Data exchange based on XML.

Shared Infrastructure

Physical connectivity between the ATO and the HIC's firewall is sharing a dedicated ICON link.

ATO Solution

The ATO will use the e-tax client to deliver medical expense data to the client to be verified, and returned as part of the Income Tax return lodgement. Other components have been added to the e-tax server environment to enable access to Claim data from the HIC Web Service and to pass it to the client on request.

ATO e-tax Client

The e-tax client is a legacy ATO application consisting of client software to fill in and lodge an Income Tax Return Form, and server components to manage authentication of the client, download of software and data, and to receipt Income Tax Lodgements from the client.

Data is encrypted between the client and the server, travelling over TCP/IP and using HTTP/S and HTML.

ATO Service Manager/Security Gateway

This .Net Active Server Page receives the request from the e-tax software and performs data and security checks before invoking the interface service that routes the request to the HIC.

ATO Interface Service

This .Net Web Service acts as a router to the HIC and calls the HIC e-tax Web Service. When the HIC responds, the interface service encrypts the HIC data, which is forwarded to the e-tax client software via the Service Manager.

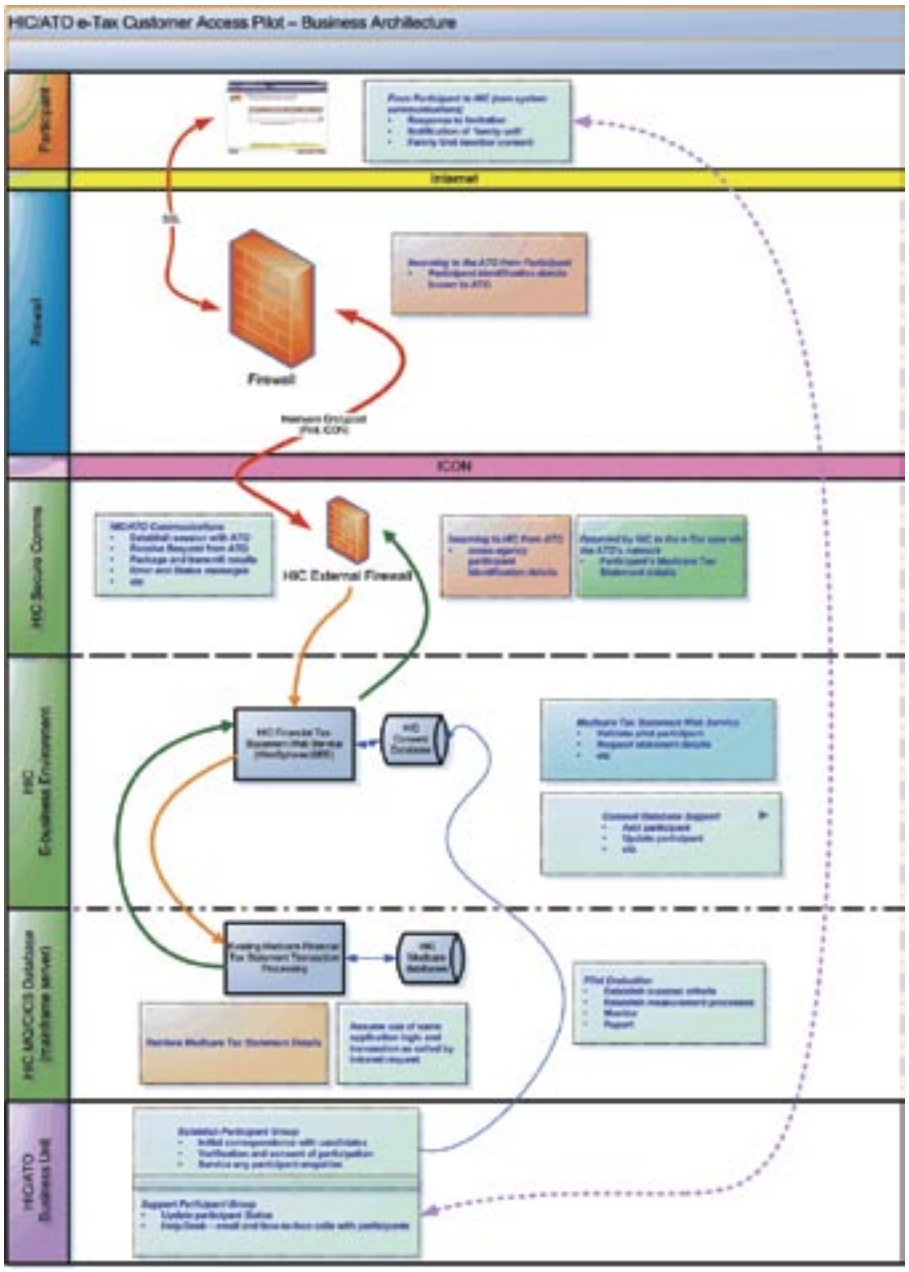
Mapping e-tax to Interoperability Framework

The following section maps the e-tax interoperability functionality against the categories described in the AGTIF, and shown below.

e-tax Solution AGTIF Mapping

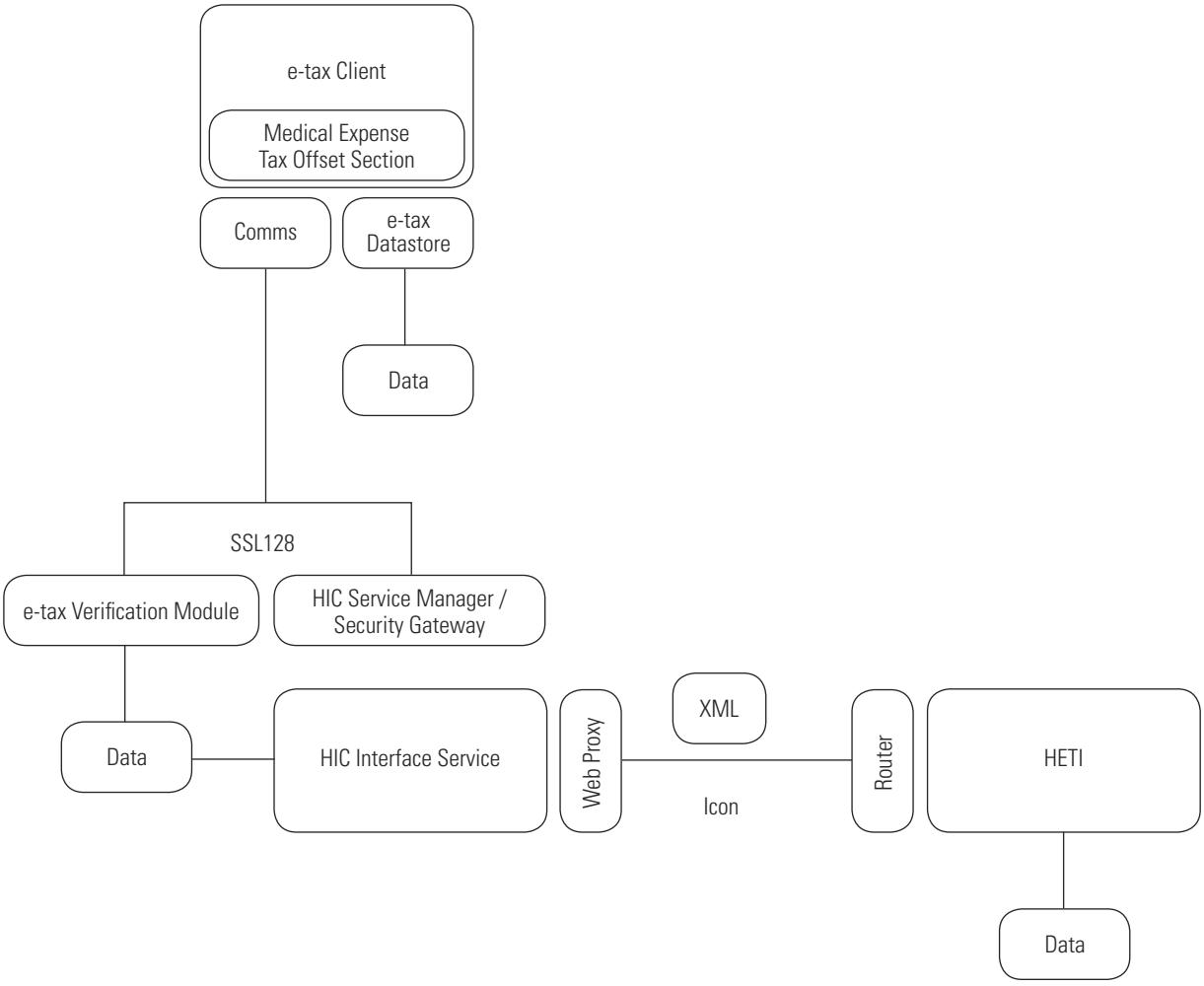
AGTIF Category	HIC	ATOTax Office	Shared	Comments/Issues
Security	The HIC Web Service is only available to the ATO over a secure dedicated line. Other components of the HIC internal solution are protected, and only available to authorised staff.	SSL 128 bit PKI used for encryption. Authentication is based on allocation of a Reference number to ATO participants, and authentication by ATO for e-tax. Data encrypted on ATO file servers.	Hardware encryption over ICON.	HIC has leveraged the ATO infrastructure to provide taxpayer authentication and connectivity.
Discovery	Not applicable	Not applicable		
Interconnection	SOAP WSDL HIC Service provided as WebSphere Web Service using HTTP/S protocol.	ISA Proxy client-server via e-tax communication module sending data as HTTPS request. .NET Web service (Interface Service) acts as a router from ATO to HIC. Service Manager performs security checks and data validation. It also assembles HTTP/S response to client and sends.	ICON	ATO components of interface (Service Manager, Interface Manager) have been built to manage connection between e-tax software and HIC Web Service.
Data Exchange	Producer of Web Service (XML, SOAP, WSDL)	Consumer of Web Service (XML, SOAP, WSDL)	XML format has been designed specifically use by partners in the pilot.	Transformation of HIC data occurs at e-tax client (from HIC semantics, to ATO semantics). XML message has been designed to meet needs of pilot, and may need further design and standardisation for a full production release.
Presentation	JSP/Java	HTML for acquiring e-tax download.		
Process modelling	Not applicable	Not applicable	Not applicable	
Data modelling	Not applicable	Not applicable	Not applicable	
Naming	HIC standard naming conventions	ATO agreed to consume service based on HIC standards.	Not applicable	HIC naming conventions are accommodated in the model.

System Architecture – HIC View



System Architecture ATO View

The newly developed system will automate the process of entering Medicare medical expenses for the taxpayer and all eligible dependants. This process is embedded in current e-tax functionality. The taxpayer will use the auto-complete function of the Medical Expense Tax Offset section (T9). This function connects to the ATO server to download the financial statement.



4.2.5 Security & Rollout

The nature of the information that is the focus of the interoperation is of a personal nature, and therefore maintaining the integrity and privacy of the data has been a major project focus. The HIC has viewed this project as an opportunity to build upon the secure Government-to-client relationship that the ATO implements via the e-tax client software. It has been the HIC's goal to leverage the ATO's existing client authentication approach rather than duplicate it. The interoperability design physically links the HIC to the ATO, while reusing the link between the ATO and the e-tax client.

The business model for this process involves providing Medicare financial information for a group of people to one requesting individual for inclusion in that individual's tax return. Typically, though not exclusively, this is a family group, and is determined according to ATO rules. The requesting individual must have permission to receive the

Medicare financial information for other group members. This is addressed by implementing a registration process, through which consent from group participants is collected and stored for later use during the e-tax process. The individuals who register for the pilot will be issued with a participation number that will be requested through the e-tax process and used by the HIC to verify identity.

Both the HIC and the ATO operate computer networks that contain sensitive data. It has been a major design imperative that the new e-tax channel does not undermine the security of the existing networks. Within the HIC, this has involved implementation of an Extranet domain for this project, which is segregated from the HIC's existing Internet and Intranet domains by firewalls, hardware and software layers.

Consent Registration is enabled through an internal HIC application. The standard HIC authentication mechanisms for Intranet applications will be used for this component.

The HIC will "trust" the ATO to authenticate users to minimise the need for additional security mechanisms at the HIC end. The HIC will not require users to re-authenticate once the ATO has established their identity.

4.2.6 Issues and Lessons Learned

This case study was prepared in late June 2004, just prior to the scheduled launch of pilot and as a consequence many of the anticipated findings of the project will emerge during the tax lodgement period from July to October 2004. Various other lessons have been learned during the development phases. Some of the areas of significant interest that this project offers to the HIC include:

- It provides an opportunity for the HIC to explore development of a *Client Service Consent Model*.
    - A Client Service Consent Model, with opt-in and opt-out provisions was developed to support the data interchange between the HIC, the ATO and the participants of the pilot. The purpose of this consent model is to address privacy issues. This will provide the HIC with an understanding of the practicalities of this model, including the level of consumer acceptance, effort and cost.
- It provides an opportunity to explore the challenges of integrating the HIC's technologies with an organisation that operates a substantially different technology base.
    - At a technical level the pilot will connect the disparate e-business architectures of the HIC (J2EE and IBM Websphere Application Server) and the ATO (Microsoft .Net) environments and leverage the HIC investment in mainframe processing by exposing the Financial Tax Statement transaction as a web-service.
    - It was anticipated at the commencement of the project that variations in the approaches of IBM and Microsoft may cause integration complexities, however this was not the case in the HIC's view. The lesson learned in this instance is that a well-defined business relationship between agencies coupled with a well understood interface has allowed the two parties to interoperate successfully.
    - Given a more complex problem however, technology differences may have been more problematic.
- It provides the opportunity to explore the challenges of integrating the HIC's information models and business processes with an organisation using different business rules and information model.
    - The Web Services solution that the HIC delivered was designed based on the HIC's information models, which differs from the ATO. These range from simple differences in data element naming conventions, through to variations in definitions of a family group from the Medicare perspective in comparison to the ATO view.
    - While technology such as XML can quite easily solve simple data transformations due to different field naming conventions, the issues such as varying business perspectives of information need to be resolved at the business level and there may be further design work required to resolve these differences.

- It provides the opportunity for the HIC to measure consumer interest in this form of service delivery.
    - The HIC is keen to measure the level of consumer interest and acceptance in delivering services through the Internet, and through non-HIC channels such as e-tax. To date, the response to invitations to participate in the pilot has been strong; however actual usage rates and patterns will not be known until the end of the tax lodgement period. Consumer usage patterns will be tracked through the pilot and will be analysed to determine the usage distribution around the clock.
- It provides the HIC with an opportunity to explore the potential to leverage and exploit whole-of-government work by other Commonwealth Agencies.
    - This project has allowed the HIC to leverage the ATO's relationship with the e-tax user base. The HIC acknowledges that the ATO has several years of experience and investment in providing secure services to consumers over the internet, and has implemented an authentication and identification model to do this.
    - From the HIC perspective, the pilot has shown that cross government interoperability appears viable and is capable of reducing red tape to deliver on a whole-of-government basis.
- It provides the HIC with an opportunity to explore Web Services technology, and the ATO to explore issues raised by consumption of other Agencies' services.
    - This project was viewed by the HIC as an excellent opportunity for the HIC to explore and pilot externally facing Web Services. The HIC decided to factor out some of the complex security and privacy aspects of interoperability by restricting access to the ATO through an Extranet-style connection over a dedicated ICON link. This approach has allowed the HIC to focus on key business problems such as the consumer consent model. While acknowledging that the product built by the HIC has not been deployed as a publicly available and discoverable Web Service, it has however provided the HIC with valuable experience in building and deploying an outward-facing Web Service.
    - If this project is extended to a full implementation in 2005, or if faced with similar cross-government opportunities, the HIC may explore options for exposing Web Services across the internet.

5. Glossary

Agency An Australian Government entity.

AGIFT Australian Governments' Interactive Functions Thesaurus, for functional description of records, information resources and services.

AGLS Australian Government Locator Service 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.

DNS Domain Name System, allows naming and location of Internet sites.

ebXML e-business XML is a joint project of the UN and OASIS to develop an XML standard for business-to-business trade.

Fedlink Is a Virtual Private Network that provides secure and trusted communications across the Internet.

FTP File Transfer Protocol, allows transfer of files between computers over the Internet. FTP is an application protocol.

GML Geography Markup Language, based on XML.

Guideline A statement of desired, good or best practice.

HTML Hypertext Markup Language is the set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page.

HTTP Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files on the World Wide Web. HTTP is an application protocol.

HTTPS HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) 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.

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

Service delivery 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 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 AGLS and its extensions and ANZLIC (geo-spatial).

MIME MIME (Multi-Purpose Internet Mail Extensions) 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 The 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.
UDDI	Universal Description, Discovery and Integration (UDDI) provides directory services to discover Internet-based business resources within the "web services" model.
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 is 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 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	Extensible Markup Language (XML) schema definition language for defining the structure, contents and semantics of XML documents.
XMLP	XML Protocol, formally 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.
XSL	Extensible Stylesheet Language (XSL) is the language for defining how a browser will display XML content to the user.

6. Bibliography

Name / Topic	Acronym	Reference
American National Standards Institute	ANSI	http://www.ansi.org/
Australian Government Information Management Office	AGIMO	http://www.agimo.gov.au
Australian Government Locator Service metadata standard	AGLS	http://www.naa.gov.au/recordkeeping/gov_online/agls/summary.html
C# programming language related information		http://msdn.microsoft.com/vcsharp/
Dublin Core Metadata Initiative	DCMI	http://www.dublincore.org
HL7 Healthcare Standards Organisation	HL7	http://www.hl7.org/
Institute for Electrical and Electronic Engineers	IEEE	http://www.ieee.org
International Standards Organisation	ISO	http://www.iso.org
International Telecommunications Union	ITU-T	http://www.itu.int
Internet Engineering Taskforce	IETF	http://www.ietf.org
Java programming language related information		http://java.sun.com
OASIS - The Organization for the Advancement of Structured Information Standards	OASIS	http://www.oasis-open.org/
Object Management Group	OMG	http://www.omg.org/
Open Archives Initiative	OAI	http://www.openarchives.org/
Standards Australia	SAI	http://www.standards.com.au
Unicode		http://www.unicode.org/
Unified Modelling Language	UML	http://www.uml.org/
United Nations Centre for Trade Facilitation and Electronic Business	UN/ CEFACT	http://www.unece.org/cefact/
Web Services Initiative	WS-I	http://www.ws-i.org/
World Wide Web Consortium	W3C	http://www.w3.org
Web Services References		http://www.w3.org/2002/ws/ http://msdn.microsoft.com/webservices/ http://java.sun.com/webservices/index.jsp

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

l. 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.

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).