New Zealand E-government Interoperability Framework (NZ e-GIF)

Version 3.0

23 May 2005

E-government Unit

State Services Commission

Foreword

THIS IS BEING REWRITTEN TO GO UNDER DUAL AUTHORSHIP: WARREN TUCKER – CHAIR E-GIF MGT COMMITTEE AND LAURENCE MILLER, DC, ICT SSC.

E-government is all about getting better results for people. Better results delivered by government as a whole.

Today's technology is remarkable. Networking, the Internet, telephony, mobile text messaging – all continually advancing. Electronic communication is transforming how we go about our work, how we learn, how we relate to each other. And the technology is changing the way government delivers services to its people.

Few beyond government circles know where the business of one agency begins and another ends. Nor should they have to. Frustrated citizens reaching the head of a queue only to be told they are in the wrong department is something of a comedy classic. But it is no laughing matter when it happens to you.

Fortunately, for many New Zealanders, the Internet has meant the end of queues altogether. While many government departments now provide their services electronically (e-services), today's challenge is to take an "outside – in" view. Agencies must look at the complete service New Zealanders seek – from their perspective. We in Government must work together, electronically, in a spirit of collaboration, to best deliver it.

Results that people value are the goals of the 2007 and 2010 e-government targets. Building upon the Development Goals for the State Sector announced in March 2005, the June 2007 target is to make networks and internet technologies integral to delivery of government information, services, and processes. We are well on our way. As agencies put the e-GIF into practice, back-office integration drives front-end services that are integrated, customer-centric, and efficient. And this brings us closer to the June 2010 target – government operations transformed through the use of the Internet.

The e-GIF is a fundamental tool for integrating agency services. It also helps the whole of New Zealand government stay in line with internationally agreed standards and protocols. By adopting the e-GIF, agencies will keep the Internet and related technologies working for New Zealanders today and in the future.

One note of caution: to be of value, the e-GIF must be used; and to be useful, it must stay relevant. I encourage all to supplement the e-GIF: submit new standards relevant to your sector – and to others, including the public sector. By working together, we can continue to enhance the e-GIF as a central repository of agreed e-government standards. And that is an all-of-government asset of considerable value.

State Services Commissioner

Contents

PART I: STANDARDS

This part contains the actual standards that make up the E-government Interoperability Framework. Its intended audience includes:

- State Sector Information Technology (IT) strategists
- Technical Analysts
- Programme and Project Managers
- anyone planning services requiring interoperability.

This part includes the following sections:

1 What is the e-GIF?

The E-government Interoperability Framework (e-GIF) is a set of policies, technical standards, and guidelines covering ways to achieve interoperability of public-sector data and information resources, information and communications technology (ICT), and electronic business processes. It creates the ability for any agency to join its information, ICT or processes with those of any other using a predetermined framework based on "open" (i.e., non-proprietary) international standards.

The e-GIF performs the same function in e-government as the Road Code does on the highways. Driving would be excessively costly, inefficient, and ineffective if there were a need to agree on road rules each time one vehicle encountered another.

1.1 What is e-government?

E-government is all about government agencies working together to use technology so that they can better provide individuals and businesses with government services and information. It is not a massive IT project. Much of it is about establishing common standards across government, delivering services more effectively, and providing ways for agencies to work together using technology.

E-government presents New Zealand with some tremendous opportunities to move forward in the 21st century with higher quality, cost-effective, government services and a better relationship between New Zealanders and their government.

For the latest version of the New Zealand e-government strategy, see http://www.e-government.govt.nz/programme/strategy.asp.

1.2 What is interoperability?

The December 2001 New Zealand E-government Strategy defines interoperability as, "the ability of government organisations to share information and integrate information and business processes by use of common standards".

The June 2003 E-government Strategy Update underscored that point, "Common data and information technology policies and standards underpin the service delivery architecture and are integral to the E-government Strategy."

From a technical standpoint, interoperability is achieved when the coherent electronic exchange of information and services between systems has taken place.

For e-government in New Zealand, interoperability relates specifically to the electronic systems that support business processes:

- between agencies
- between government and people
- between government and business.

This does not mean that a central agency is simply dictating common systems and processes. Interoperability can be achieved by the application of a framework of

policies, standards and guidelines that leave decisions about specific hardware and software solutions open for individual agencies or clusters of agencies to resolve.

This document sets out the framework.

1.3 What will the e-GIF accomplish?

Use of the e-GIF:

- helps government agencies more easily work together electronically
- makes systems, knowledge and experience reusable from one agency to another
- reduces the effort required to deal with government online by encouraging consistency of approach
- reduces the reliance on tapes and disks to exchange data, since these carry their own security issues and are not scaleable for the level of interoperability many services will require in future.

Practical example: consolidating customer resources

In practice, adherence to the e-GIF becomes critical when two or more agencies work together to deliver a service online. Agencies are encouraged to look at services from a "customer" perspective.

A hypothetical example might be "opening a café/restaurant". Today this involves interactions with:

- the Companies Office for a company number and IRD-GST number (until very recently you had to go separately to the Inland Revenue Department for an IRD number)
- Occupational Safety and Health (OSH) Accident Forms, Hazardous substance policy, etc.
- Accident Compensation Commission (ACC) for Levy forms and Workplace Safety policy, etc.
- the local council for signage, a certificate of food hygiene, etc.

Today, most of this information is available online – but only by visiting each agency's website for its respective services. Consider our fictitious example in an interoperable future: all services for opening a café/restaurant, delivered by multiple agencies, available through a single website: http://www.openingmycaferestaurant.govt.nz . The applicant would enter relevant details; and the agencies would exchange relevant information amongst themselves and the applicant to supply all the required services.

This is the kind of interoperability envisaged in the next phase of e-government. To accomplish such interoperability, the agencies need an enduring, agreed standard set for exchanging data between all parties. The e-GIF sets forth these standards.

(See also Section 6.2, Aims of the e-GIF.)

1.4 Managing the e-GIF

Stewardship

The following people manage the e-GIF:

- The **State Services Commissioner** is the **Steward** of the e-GIF, having accountability and corresponding decision-making authority for its ongoing development and management.
- The **E-government Unit (EGU)** of the State Services Commission is the **Custodian**, with responsibility for the day-to-day operation of the e-GIF under the oversight of the **e-GIF Management Committee**.
- The **e-GIF Management Committee** comprises public servants from the senior ranks of agencies adopting the e-GIF.
- **Working groups** are established to regularly review the technical aspects of the e-GIF.
- All **agencies** that are required to adopt the e-GIF may participate in its governance and appeal decisions made by the Steward and Management Committee.

Who to contact

You can contact the custodian at e-gif@ssc.govt.nz.

2 Who must comply and when?

The e-GIF is a forward-looking document. It specifies a set of standards to be applied when developing or upgrading technology. This section outlines who must and who is encouraged to comply; how to make the transition; and how to apply for an exemption.

2.1 Who must or is encouraged to comply

Mandatory compliance

From 1 July 2002, Cabinet has made use of the e-GIF **mandatory** for:

- all Public Service departments
- the New Zealand Police
- the New Zealand Defence Force
- the Parliamentary Counsel Office
- the Parliamentary Service
- the Office of the Clerk
- the New Zealand Security Intelligence Service.

Suggested compliance

The benefits of the e-GIF are not specific to the Public Service or central government. Cabinet has **encouraged** adoption by:

- organisations in the wider State sector
- local authorities.

The e-GIF is also open to use by:

- non-government organisations
- the business community
- the public
- other jurisdictions.

2.2 How and when to comply

In general, all organisations who must or are encouraged to comply with the e-GIF (see Section 2.1), should review their implementations against the e-GIF whenever:

- a new version of the e-GIF is released
- they are contemplating new implementations
- they are contemplating upgrading implementations
- they are reviewing their overall technology strategy.

For details, see below.

Transitions

The adoption of the e-GIF must allow for a sensible transition. Recognising this, on 13 June 2002 Cabinet agreed that current information systems, software applications, or electronic data/information resources do not need to immediately comply with the NZ e-GIF.

Any new information system, software application, or electronic data/information resource (or current instances of these being redeveloped or replaced); or systems for interfacing with the same; must comply with the e-GIF except in instances where:

- it is certain that interoperability will never be a requirement; or
- the current version of the e-GIF does not, and could not, include policies, standards or guidelines concerning the technologies the agency needs (not wants) to employ.

If a reader believes their agency has one of these exceptional instances, please remember to consider the "outside-in" view (see the Practical example: consolidating customer resources on page 7). Although the agency system may have been developed to operate in isolation, New Zealanders may one day need it – transparently or otherwise – to work with other services from other agencies. Is it absolutely certain that the new system, application or resource will *never* need to support or interact with any new, enhanced, or replacement system, application, interface, service, process, or resource? Experience shows that in the vast majority of cases, the e-GIF will apply.

Information sharing and matching agreements

In many (but not all) circumstances, interoperability requires the exchange, sharing, or matching of personal information. The Privacy Act may well apply in these situations, particularly Part 10 and schedules 3 and 4; and for information-matching programmes, the Act mandates a Technical Standards report.

Agencies planning data exchange are encouraged to:

- contact the Office of the Privacy Commissioner regarding the circumstances of the exchange (it may fit with one of the 31 information-matching programmes authorised by Parliament)

- review their existing (offline) data-management agreements and:
  - extend them to include issues relating to electronic exchange
  - add them to the Technical Standards Report
  - or prepare new agreements or Memoranda of Understanding.
- seek legal advice.

See also:

- Section 6.3, Governance of shared inputs
- Section C.5, Information Systems and Data Management Policies and Standards
- Checklist for data exchange issues to be covered in a Memorandum of Understanding (MOU) or data sharing agreement – please email e-GIF@ssc.govt.nz for access to this document.

2.3 Exemptions

Where an agency believes there are grounds for exemption from the e-GIF, it must:

- conclusively demonstrate, to the satisfaction of the e-GIF Steward, where the current version of the e-GIF cannot meet requirements or why an alternative approach to achieving interoperability is justified; and
- where sensible, contribute to the updating of the e-GIF.

Where an exemption is approved, it will apply *only to a specific:*

- information system, software application, data/information resource, or business process (not to the agency's entire information and technology environment and/or business processes)
- agency or agencies (not to an entire sector)
- time period (not indefinitely).

For more information, including a template for applying for an exemption, see http://www.e-govt.govt.nz/interoperability/faq.asp.

Special provisions

Specialist systems employed by or sponsored by the security and intelligence agencies are automatically exempted where it is not appropriate to comply with the e-GIF.

3 How to read the standards

The e-GIF standards are formatted in tables broken down using a "layer model", structurally categorizing technology. Each table includes standards, with version numbers where applicable, a status, review cycle, and comments. This section explains how to read the tables.

3.1 Layer model

Layer models are widely used to classify functions within IT systems. The intent is to simplify systems by segregating system functions into levels and disentangling the complexity and variations of each level. Components normally communicate only with others at neighbouring levels, and in standardised ways.

The model for this version of the e-GIF is illustrated and described below.

Figure 1: e-GIF v3 Layer Model

The four basic structural components (layers) of this model are:

- **Network** – Covers details of data transport such as network protocols. This is a crucial area for interoperability. Without agreement on networking standards it is hard or impossible to make systems communicate. The e-GIF uses a subset of the widely proven Internet Protocol suite.
- **Data Integration** – Facilitates interoperable data exchange and processing. Its standards allow data exchange between disparate systems and data analysis on receiving systems.
- **Business Services** – Supports data exchange in particular business applications and information contexts. Some of the standards in this layer are generic, covering multiple business-information contexts; others work with data-integration standards to define the meaning of the data, mapping it to usable business information. For example, an agency will format a stream of name-and-address data in XML (Data Integration) using the business rules of xNAL

(Business Services) to create a commonly agreed representation of name-and-address information.

- **Access and Presentation** – Covers how users access and present business systems. Most of the standards in this layer are in the Government Web Guidelines.

Applying to all of the structural layers are:

- **Security** – Crosses all layers, to reflect the fact it needs to be designed into a system, not added as a layer on top. The e-GIF contains standards at the various levels designed to offer different levels of security as appropriate. It also refers to a series of standards and policy statements (the NZSITs) which provide advice and direction on the levels required.
- **Best Practice** – New category to help readers of the e-GIF distinguish published standards from Best Practice, Codes of Practice, and other general or sector-focussed guidance. Published standards alone do not ensure interoperability – they merely offer a common approach to managing and understanding the context of the information exchange.
- **E-government Services** – These are actual implementations of IT infrastructure made available by the EGU for use by public-sector agencies. (See Section 5, E-government services.)
- **Web Services** – An emerging set of standardised applications to connect and integrate web-based applications over the internet. *Web Service*s connect *services* together. Using Best Practice implementations, agencies can agree a common approach to interoperable service delivery to customers.

Underpinning all layers are:

- Management – See Section 1.4 Managing the e-GIF.
- Governance – See Section 1.4 Managing the e-GIF and Section 6.4 Governance principles. An e-GIF Governance overview paper is also available from the SSC EGU. Please email e-GIF@ssc.govt.nz for access to this document.

3.2 Compliance status levels

The status level of an e-GIF standard indicates its maturity relative to other standards. In 2004, the e-GIF Management Committee agreed revised status levels for e-GIF standards. The Committee renamed Mandatory and Recommended levels and extended them to include: Adopted, Recommended, Under Development, and Future Consideration. The revised statuses broadly align with the levels used in the UK e-GIF[1]. The requirement for an additional category, Deprecated, became self evident in 2005.

The e-GIF does not require a standard to pass through each successive stage of development. When the Committee publishes an e-GIF standard, they give it an appropriate status. When the standard matures, the Committee can consider recommendations to alter its status.

[1] The criteria for status levels have been adapted from the UK e-GIF Interoperability Working Group draft paper "Criteria for TSC standards V1.doc".

Current e-GIF compliance statuses

The current e-GIF standard compliance status levels are illustrated and described below.

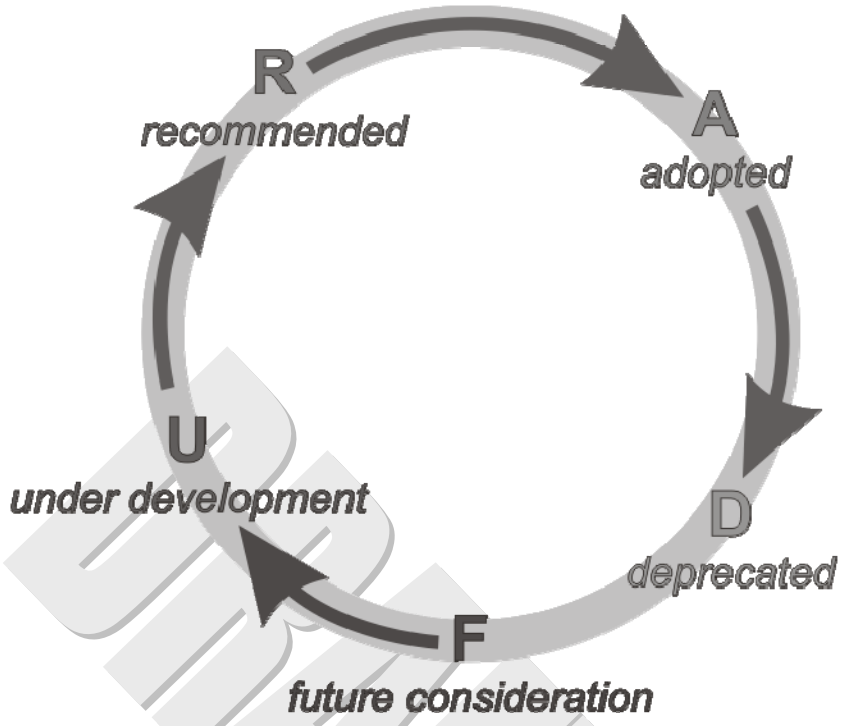

Figure 2: e-GIF Compliance Status Cycle

The compliance statuses in this version of the e-GIF are:

- **Future Consideration** (**F**): – not yet reviewed, customised, nor having any successful, documented implementation in the New Zealand government; yet probably necessary for public-sector IT systems. Included mainly to introduce to IT developers. F-level standards are:
  - possibly required for interoperability of IT systems in the public sector
  - open or demonstrating the intention of being open once published
  - not overruled by an existing international standard
  - not clashing with or rival to a standard already listed.

- **Under Development (U)**: – actively under assessment by more than one government agency; for example, having an active working group, a proof of concept, or a pilot implementation with associated documentation. Active or starting within three months of publication. U-level standards are:
  - required for interoperability of IT systems in the public sector
  - open or demonstrating the intention of being open once published
  - not overruled by an existing international standard
  - not clashing with or rival to a standard already listed
  - published or very soon to be published.

- **Recommended (R)**: – emerging from the development, review, or working-group process with implementation documentation and evidence of successful interoperability and data exchange. Recommended standards are generally more recent, founded upon newer technologies or standards. R-level standards are:
  - required for interoperability of IT systems in the public sector
  - open
  - scalable
  - not overruled by an existing international standard
  - not clashing with or rival to a standard already listed
  - complete and published
  - showing clear indication of market support.

- **Adopted (A)** – mandatory; normally upgraded from Recommended status (only in exceptional circumstances can a standard enter the e-GIF as Adopted without first completing a successful period as Recommended). A-level standards are:
  - meeting or surpassing all criteria from the previous status levels
  - well established in public-sector ICT systems
  - having complete supporting documentation and processes for implementation
  - proven effective for interoperability.

- **Deprecated (D)** – a standard or practice that has been abandoned for or superseded by a better solution in the Adopted or Recommended levels. Agencies should plan to migrate away from solutions assigned with this designation as soon as practical. New use of this standard is discouraged.

Choosing between standards – agency considerations

Given the need to maintain the e-GIF, to keep pace with changing technology, multiple standards may be available for an particular application. Agencies collaborating on interoperability projects may need to either agree one standard or use mapping technologies to achieve interoperability.

When choosing a standard:

- first consult with agencies whose functions and services relate to your own (your likely interoperability partners)
- then together agree a standard, considering the compliant statuses:
  - use **R** (recommended) standards if you can; they are generally newer and less subject to obsolescence than **A** standards
  - if you cannot or do not wish to use **R**, use **A** if you can
  - if you cannot use **R** or **A** standards, use any applicable **F** or **U** standards *and notify the SSC EGU* for Working Grouping information and to document your implementation as part of the standards-development process

- if no current standards apply, or you wish to propose a new standard, first please contact the SSC EGU for Working Group information
- avoid new use of **D**.

Note that there may be circumstances where agencies agree to use a more mature standard (e.g., **A**) over one that is likely to have a longer life cycle (e.g., **R**). They may also accept the risk of a newer standard (e.g., **F** or **U**) instead, with the understanding that that they will be participating in its development.

3.3 Links

Standards included in the e-GIF that are blue and underlined have links to an RFC or other resources on the Internet, which more fully explain them. If you are using a hard-copy version of this document, see Appendix D, URLs referenced in this document.

3.4 Comments

The comments column provides additional information on the background, circumstances of use, or anecdotal feedback that may help agencies in their decision to use or implement the applicable standard.

3.5 Changes from previous version

The following elements of the standards tables are new to e-GIF version 3.0:

- **Statuses** – version 2.1 standards were either Mandatory or Recommended; this version uses the scheme described above.
- **Columns** – tables now include columns for Status, and Comments.
- **Web Services Section –** standards specifically related to Web Services implementation that do not strictly fit into the layer model.
- **Best Practice Section** – standards that do not strictly fit into the layer model but rather apply in a particular context only.
- **Added, moved, removed, revised standards** – see the Change Log in Appendix B, History of the e-GIF.

4 e-GIF standards

This section sets out the current and emerging standards required for e-GIF compliance and to facilitate interoperability. The abbreviations used in this section are spelt out at the end of the document. Links in the tables to online resources (usually the standards themselves) explain more fully what each covers; see also Appendix D, URLs referenced in this document. For a list of standards that are new, moved, removed, or changed in this version, see Appendix B, History of the e-GIF.

4.1 Network layer

This section covers details of data transport such as network protocols, which is a crucial area for interoperability. Without agreement on networking standards it is hard or impossible to make systems communicate. The e-GIF uses a subset of the widely proven Internet Protocol suite.

Component	Standard	Status	Comments
Network Protocols (TCP/IP)	TCP	A	Transmission Control Protocol.
	UDP	A	A lower service level alternative to TCP, User Datagram Protocol offers minimal transport service for applications using multicast/ broadcast delivery, DNS, routing information, and network management. Omission from previous version.
	IP Version 4	A	Plan for migration to IPv6. New hardware should support IPv4 as well as IPv6.
	IP Version 6	R	When implementing IPv6, configure routers to "ghost" IPv4.
Directory	LDAP Version 3	A	For access to directory services.
File Transfer	FTP	A	Use restart and recovery. Also FTP security extensions and FTP via Port 80 where applicable.
	HTTP Version 1.1	A	Application-level protocol. See Section 4.6, Security layer for secure HTTP (HTTPS) and TLS usage.
	WebDAV	F	World Wide Web Distributed Authoring and Versioning is a set of extensions to HTTP1.1 that allows users to collaboratively edit and manage files remotely but avoids access problems with NAT firewalls.
	SCP	F	SCP is a simple protocol which lets a server and client have multiple conversations over a single TCP connection. The main function of SCP is the secure file transfer between a local and a remote computer. It uses Secure Shell (SSH) and supports Secure FTP.
Mail Transfer	SMTP	A	Host-to-host protocol. Beware of spoofing of email addresses. SMTP-TLS is used to protect mail headers

Component	Standard	Status	Comments
Registry Services	DNS	A	Use DNS for Internet/Intranet domain to IP address resolution. DNS Security is critical. Omission from previous version.
Time	NTP Version 4	U	De facto standard proposed for use in an all-of-government time standard. Best practice guidelines are being developed
	UTC (MSL)	U	De facto standard (accessed from Industrial Research Limited, Measurement Standards Laboratory (MSL)); proposed for use in an all-of-government time standard. Best practice guidelines are being developed
Messaging Transport	HTTP Version 1.1	A	See File Transfer above and Section 4.6, Security layer.
Messaging Formats	MIME	A	See also S/MIME and Section 4.6, Security layer for secure mail attachments. Do not use Transport Neutral Encapsulation Formats (TNEF) for headers.

4.2 Data Integration layer

The Data Integration layer outlines the standards in the realm of data exchange and processes.

Component	Standard	Status	Comments
Primary Character Set	ASCII	A	Minimum set of characters for data interchange. Omission from previous version.
	UTF – 8 bit encoded	A	Unicode Transformation Fomat is an extension of ASCII.
Structured Web Document Language	HTML Version 4.01	A	For web content. See Web Guidelines Version 2.1.
Schema Definition Languages	XML Version 1.0	A	Meta language to create tags to define, transit, validate, and interpret data.
Document Type Definition	DTD	A	Describes multiple elements and attributes for XML; see W3School's DTD Tutorial.
Structured Data	XML Version 1.0	A	
Batch/bulk Data	CSV	D	XML 1.0 is strongly preferred for structured data transport. Parties must agree file header records before exchange. Omission from previous version.
File Compression	ZIP Version 2.3	A	Other products using the compression algorithm LZH are also acceptable, subject to the agreement of the exchanging parties.
	GZIP	A	Not compatible with ZIP. Omission from previous version.
File Archiving	TAR	A	Omission from previous version.

4.3 Business Services layer

Business services describe the services and data from a business point of view, i.e. mapping the technical components to useful business information.

Component	Standard	Status	Comments
Metadata (Discovery)	NZGLS Version 2.0	A	
	NZGLS Thesauri	A	
	RDF	A	Resource Description Framework is an XML file format to describe metadata. RDF is used by RSS1.0 (see later in this section).
Namespace	URN	U	Working group to be led by SSC EGU See also Internet Draft.
Schemas	W3C schema definitions	A	Use when other schemas customised for use by government agencies are not specifically identified (e.g., NZGMS, xNAL (nz), NZGLS).
Structured data description	XML Version 1.1	A	Erratum in previous version.
Name and Address	xNAL Version 2	A	xNAL (OASIS) Version 3 being drafted; will be incorporated into e-GIF following a successful pilot.
	xNAL (nz) schema	R	Agency User Group led by SSC EGU; xNAL (nz) will ultimately be replaced by xNAL (OASIS) Version 3.
Additional Customer Information	xCIL	F	The superset of xNAL specifying formats for customer information elements such as phone and fax number, email address, date of birth, gender, etc. xCIL is already under consideration by several agencies and is being piloted in the web-based Change-of-Address Notification project
	Data formats for identity records standard	U	The All-of-government Authentication project is using schema fragments from xCIL to develop the Identity Records standard. This specifies data formats for a range of customer-information data elements that government agencies may use in customer identity records.
Customer Relationship	xCRL	F	Part of the xCIL and xNAL family of standards specifying formats for relationships between customers.
e-Learning	ADL, SCORM, and IMS	F	Specifications currently being considered by the E-learning Working Group.
Business Reporting	xBRL	U	Working Group underway, led by IRD.

Component	Standard	Status	Comments
Directory Services	DSML	F	Directory Services Markup Language.
Statistical Data and Metadata	SDMX	F	Statistics New Zealand leads this standard.
Geospatial	GML	A	Land Information New Zealand leads this standard.
	WFS	A	Land Information New Zealand leads this standard.
	WMS	A	Land Information New Zealand leads this standard.
	ESA	R	Emergency Services in government Administration. Land Information New Zealand leads this standard.
	NZGMS	R	Schema for identifying geospatial metadata. Land Information New Zealand leads this standard.
Registry Services	ebXML RIM and RS Version 2.1	A	Open standard application for Registry Information and Records Services in an e-business context, as an alternative to Web Services.
	ebXML RIM and RS Version 3.0	F	Open standard application for Registry Information and Records Services in an e-business context, as an alternative to Web Services.
Content Syndication and Channel Feeds	RSS	R	Note that this standard is required for agencies using the government portal news service (see Section 5, E-government Shared Services).
Instant Messaging	XMPP	F	XML protocol for real-time messaging. Taken from UK Technical Standards Catalogue Version 6.2.
Voice Over Internet Protocol	H.323 Version 2	F	Taken from UK Technical Standards Catalogue Version 6.2. Codec required.
	SIP	F	SIP has greater take-up than H.323. Session Initiation Protocol. Taken from UK Technical Standards Catalogue Version 6.2. Codec required.

4.4 Access and Presentation layer

This section presents standards and guidelines covering how business systems are presented and accessed by users.

Component	Standard	Status	Comments
Website Presentation	NZ Govt Web Guidelines Version 2.1	R	See Web Guidelines 2.1 for use of: HTML 4.01, XHTML, GIF 89a, JPG, PNG, SVG, and PDF.
Web design and maintenance	NZ Govt Web Guidelines Version 2.1	R	Proposed change to Adopted status in 2006.
Forms	xForms	F	Open standard for use of XML forms on web pages, to replace HTML forms.
Authentication Standards ***Note:*** *Agencies wishing to implement any new systems where authentication of individuals or businesses is necessary must contact the SSC EGU for advice.*	Evidence of identity standard	U	Specifies a business process for establishing the identity of government-agency customers.
	Username / passwords standard	U	Specifies use of username/passwords for online authentication.
	"Key type 2" standard	U	Specifies use of an as-yet-undefined key type for online authentication.
	Authentication key strengths standard	U	Specifies and populates a model for comparing the relative strengths of authentication keys.
	Trust levels for online transactions standard	U	Maps online transactions to authentication key strengths and evidence-of-identity confidence levels.

4.5 Web Services layer

Web services are an emerging set of standardised applications to connect and integrate web-based applications over the internet. The e-GIF identifies them separately, as they span multiple parts of the layer model. It is critical that agencies using web services agree on the implementation and semantics of data. The emergence of the WS-I Basic Profile 1.1 offers a starting point for a consensus on web-services implementation across government.

The following standards apply where systems use a web-services architecture.

Component	Standard	Status	Comments
Discovery	UDDI Version 3	A	An open standard for describing, publishing, and discovering network-based software components.
Description	WSDL Version 1.1	A	Web Services Description Language specifies the location of the service and the operations (or methods) the service exposes.
Access	SOAP Version 1.2	A	For Web Services Transport.
Messaging	ebXML MSG	F	Also known as ebMS.
	AS2	F	A lightweight, open messaging transport for B2B messaging services. Comparable with ebXML MSG/ebMS.
Security	WS - Security	F	Security standard under development by OASIS.
	SAML Version 2.0	F	Secure messaging and security token framework. A subset of SAML 1.1, elements are Under Development as part of the All-of-government Authentication project. See Section 4.5, Access and Presentation layer. OpenSAML is an implementation of SAML.
	xACML Version 2.0	F	XML Schema for creating policies and automating their use to control access to disparate devices and applications on a network.
Compliance	WS-I Basic Profile Version 1.1	F	Profiles provide implementation guidelines for how related web-services specifications should be used together for best interoperability. To date, WS-I has finalized the Basic Profile, Attachments Profile and Simple SOAP Binding Profile.
	WSS-I Basic Profile Version 1.0	F	Draft 1.0 Basic Security Profile accepted by OASIS.

4.6 Security layer

Security is shown in the e-GIF as spanning all layers to reflect the fact that it needs to be designed into a system, not added as a layer on top. There are four main contexts in which security can be viewed:

- confidentiality – ensuring that information is accessible only to those authorised to have access
- integrity – safeguarding the accuracy and completeness of information and processing methods
- availability – ensuring that authorised users have access to information and associated assets when required
- accountability – the ability of a system to keep track of who or what has accessed data, conducted transactions, or made changes to the system. [2]

Agencies are encouraged to consider the Security implications of interoperability projects using these contexts, and apply the appropriate policies and standards. The following table contains standards designed to offer different levels of security in the layers; the standards and policy statements in the NZSITs provide advice and direction on what levels may be required.

Component	Standard	Status	Comments
Policy	GCSB NZSITs	A	Please note that the NZSITs are currently being updated. Refer to GCSB for advice on hashing, key transport, signing, and cryptographic algorithms currently in the draft revision to the NZSIT400.
	SIGS	A	Security in the Government Sector is a policy-and-standards guideline largely drawn from ISO 17799.
Network	HTTPS	A	HyperText Transfer Protocol running over SSL. See SSL V3 below. Omission from previous version
	S-HTTP	F	Secure HTTP for individual messages, created by SSL running under HTTP.
	SSL Version 3	A	Use for encrypted transmission of any data quantity between web browser and web server over TCP/IP. Uses HTTPS (HTTP in an SSL/TLS stream) to open a secure session on Port 443.
	TLS	F	RFC 2616 upgrade mechanism in HTTP 1.1; initiate Transport Layer Security over an existing TCP connection. Does not yet interoperate with SSL V3.
	IP-SEC	A	IP Security Authentication Header standard taken from NZSIT/SIGS. Omission from previous version.

[2] Sourced form ISO17799: *IT - Code of Practice for Information Security Management.*

Component	Standard	Status	Comments
Network (cont.)	ESP	A	IP Encapsulation Security Protocol for VPN Requirements taken from NZSIT/SIGS. Omission from previous version.
Data Integration	XML - Enc	F	XML-Encryption syntax and processing. Taken from UK Technical Standards Catalogue Version 6.2.
	XML-DSig or OASIS DSS	F	XML-signature syntax and processing as defined by W3C is used in SAML implementations. OASIS Digital Signature Services is developing an alternative implementation.
Web Services	SAML Version 2.0	F	A subset of SAML V 1.1, elements are Under Development as part of the All-of-government Authentication project. See Section 4.5, Access and Presentation layer.
	Security Assertion Messaging standard	U	All-of-government Authentication Project standard Under Development. Expected to specify four specific messages from SAML for communicating authentication assertions.
Business Services	SEE PKI	R	For agencies using the Secure Electronic Environment (SEE) e-government component. See Section 5, E-government services for more details.
	S/MIME Version 3	A	Use MIME when security is not a concern. Use Secure/MIME (S/MIME) encryption when not using the Messaging Transport protocols listed in Section 4.1, Network.
	SEE MAIL	R	A combination of procedures and standards already listed in the e-GIF, required to use the e-government component SEEMail service. See Section 5, E-government services for more details.
	SecureMail	U	A combination of procedures and standards already listed in the e-GIF required to use the e-government component SEEMail service. See Section 5, E-government services for more details.

4.7 Best Practice layer

This section presents international standards and local conventions that support best practice – rather than the actual data exchange in interoperability. Agencies use these standards not necessarily with direct dependence on the standards of other agencies with whom they interoperate, but to support interoperability in general.

Component	Standard or Convention	Status	Comment
Digital Rights Management (DRM)	Do not enable.	U	See October 2004 paper on Trusted Computing. A Working Group is considering conventions for use across government.
Trusted Computing	discussion paper on Trust and Security on the Internet	U	No convention yet – see EGU Report on Trust & Security. A Working Group is considering conventions for use across government.
Process	BPEL4WS	A	Business Process Execution Language for Web Services lets users describe business-process activities as Web services and define how they can be connected to accomplish specific tasks. Omission from previous version.
XML Data Transformation	XSLT	A	eXtensible Stylesheet Language Transformations is a description vocabulary used by XSL to describe how an XML document is transformed into another XML document.
Data Modelling	UML	A	Unified Modelling Language is useful for describing objects in a visual format.
	XMI	R	XML Metadata Interchange enables easy interchange of metadata between modeling tools such as UML and remote metadata repositories.
	UBL	F	Naming and design rules for schema design.
Processing Structured Data	SAX	A	Parser for large volume repetitious batch transfers. Open standard for navigating and updating XML documents.
	DOM	R	Parser for transactional exchanges. Simple API for XML is a Java API for navigating XML documents.
Controlled Vocabulary or code Lists (CVLs)	discussion on standardising CVLs	F	Research underway, led by SSC EGU.

Component	Standard or Convention	Status	Comment
Health Sector	Privacy, Authentication and Security (PAS)	A	Health Information Management Code of Practice for Ministry of Health (MOH) and ACC. Security principles, drawn from AS/NZS ISO/IEC 17799:2001.
	HL7	U	Health Level 7 is an international standard adopted by the Health sector. Are converging on HL7 Version 2.4 for laboratory results and National Health Index (NHI).
Document File Format	ODFOA Version 1.0, DocBook, WordML	F	Several candidates for agencies to save documents in an open, XML format. The Parliamentary Counsel Office's PAL project leads this initiative.

5 E-government services

The following items comprise the e-government services. They are actual implementations of useful functions that are:

- available for re-use by government agencies
- compliant with the e-GIF.

Service	Purpose	Description
Metalogue	Services and Document Description (metadata) Database	A web-based repository for metadata, used to drive the Portal.
Portal News Feed	News Syndication	Uses NZ Government RSS to accept news items from government agencies for display on the Portal. This can also provide a feed of government news for use on agency web sites.
Authentication	Government to Individual and Government to Business online authentication	This project is in Phase 1, referred to as the Shared Logon Initial Implementation. This phase is developing and trialling a Government (also known as Shared/Common) Logon Service to help agencies authenticate New Zealanders wishing to access agency services. Agencies interested in joining the trial should contact the SSC EGU.
Shared Workspace	Online collaboration tool	Workspace is available at a modest charge for agencies to run collaborative projects in an online environment. Workspace content-management functionality includes message threading, library and archiving, alerting and news/event announcements.
Government Intranet	All-of-Government Online information repository	This is currently in pilot with a limited number of agencies before roll-out later in 2005.
SEE Mail and SecureMail	New Zealand Secure Email Requirements	Hardened email. Two domains are offered: • SEE Mail is a gateway-gateway crypto layer running over public email, improving confidentiality and authentication. Intended for use between government bodies (including local government). Note that the next version of this service will not accept UUENCODE or TNEF message formats. • SecureMail is an extension of SEEMail to the New Zealand public, via commercial Internet service Providers. Currently piloted by ACC.

Please note that government agency web search capability is under review. Agencies considering products are advised to contact the SSC EGU.

PART II: POLICY

This part outlines the policy behind the e-GIF and its development. Its intended audience includes:

- Policy Analysts
- Advisors
- Business Analysts
- and anyone involved with interoperability strategy and projects.

This part includes the following sections.

Section	Page	Description
Principles	30	Short descriptions of anticipated outcomes of the e-GIF, requirements for project management and operational management, and governance principles.
Developing the e-GIF	33	Outlines of procedures for extending the e-GIF, submitting a new standard, developing the framework; and issues under review or proposed for future working groups.

6 Principles

6.1 Outcomes for e-Government

The e-government programme seeks the following outcomes, assisted by the application of the e-GIF:

- **Convenience and Satisfaction:** services provided anytime, anyhow, anywhere; people will have a choice of channels to government information and services that are convenient, easy to use, and deliver what is wanted. This outcome will be achieved when:
  - many services are fully or partially delivered electronically (as appropriate)
  - traditional service delivery channels (counter, postal, telephone, etc.) continue to exist but are enhanced by the use of technology.

  By interoperating using the e-GIF, agencies will provide services and information electronically in the way that people want.
- **Integration and Efficiency:** services that are integrated, customer-centric and efficient; information and services will be integrated, packaged, and presented to minimise cost and improve results for people, businesses, and providers. This outcome will be achieved when:
  - front-office integration is well developed, with many services redesigned and bundled together in ways that better meet customer needs
  - back-office integration is advancing through the adoption of the e-GIF and progressive building of components of the service-delivery architecture.

  By interoperating using the e-GIF, agencies can work together electronically acting more like a single enterprise than a collection of individual agencies.
- **Participation:** people will be better informed and better able to participate in government. This outcome will achieved when:
  - online participation becomes an increasingly important part of policy development and service delivery
  - democratic processes may be electronically enabled (e.g., e-voting in local body elections).

  By interoperating using the e-GIF, agencies can make information available to people in ways that help them to participate in the processes of government.

6.2 Aims of the e-GIF

The e-GIF aims to improve the practical application of information-and-communications technologies (ICT) between the public and government, within and between agencies, and within a global context.

Improving the public face of government

People access government services largely out of need rather than choice. Their needs are seldom confined to the business of a single agency. Rather, people typically have to deal with several agencies to achieve their goals or meet their obligations.

One of the aims of the e-government programme is to make it easier for people to deal with multiple agencies by making good use of ICT. By making ICT systems and the processes they support interoperate, people will find it easier to do business with government as a whole. This does not mean that everyone has to be online to get the benefits of interoperability. If agency ICT is interoperating effectively, people dealing with public servants face-to-face or on the phone will get better service.

Improving agency use of ICT

The adoption of common technical standards for ICT means that agencies can focus more on the business outcomes the systems are designed to support than on what may be technical choices that have little impact on service delivery.

Common technical standards also mean that the collection of ICT systems across government is of more value as a whole than the sum of its parts. Disparate systems that cannot work together are only of value in and of themselves.

The adoption of common technical standards also means that, across government, knowledge of these technologies will be concentrated rather than spread more thinly across numerous alternative and often proprietary technologies.

Operating in a global environment

The Internet, and the value that it can deliver to government and people, relies on an agreed standards-based approach. By using the same standards-based approach, agencies in a small way support the infrastructure of technologies that they increasingly rely on to deliver services and conduct the business of government.

The adoption of common standards also helps governments in various jurisdictions to interoperate. This becomes important when dealing with matters that can only be handled in a regional and global way.

6.3 Governance of shared inputs

Agencies interoperate

- to make better use of ICT within government
- to deliver an integrated service directly to people or business.

In both cases collaborating agencies jointly provide inputs and must allocate the decision-making rights accordingly. Guidance on how to go about allocating decision-making rights is available from the E-government Unit.

Project management

Before committing significant expenditure on an initiative involving more than one agency, those involved should agree and put in place appropriate project management processes (see Guidelines for Managing and Monitoring Major IT Projects).

Operational management

There should be some form of agreement for on-going operation of any initiative involving more than one agency. The content of the agreement will depend on the nature of the initiative undertaken, but the following areas need to be considered:

- roles and responsibilities of each agency
- processes undertaken by each agency and the required service levels
- performance measurement for each agency's service and problem resolution
- data quality and problem resolution
- cost recovery between agencies.

6.4 Governance principles

The following principles underpin the governance of the e-GIF and its operation:

- The e-GIF will align with the E-government Strategy and the recommendations of the Review of the Centre.
- There will be a clear chain of accountability flowing from a Cabinet Minister with appropriate portfolio responsibilities.
- Adequate organisational resources and capabilities must support the governance arrangements.
- The governance arrangements will be consistent with public-sector legal requirements.
- The principles of stewardship and custodianship apply, as set out in the Policy Framework of Government-held Information [CAB (98) M 22/27 refers].
- Roles, responsibilities, and accountabilities will be clear.
- The governance arrangements will build confidence in, and commitment to, the e-GIF from all its stakeholders.
- With regard to the day-to-day operation of the e-GIF, the governance arrangements will show a close fit with the responsibilities and capabilities of the organisations involved.
- The processes for maintaining, developing, and implementing the e-GIF should be inclusive and as consensual as possible.
- The governance arrangements must account for the complexity of e-government stakeholders and operating environments.
- Agencies that are required to adopt the e-GIF will be given the opportunity to participate in its governance.
- Agencies that are required to adopt the e-GIF will have access to a process for raising concerns over decisions made by the Steward or the Management Committee.
- The collective interests of government should be balanced with the interests of individual agencies and their stakeholders. Where this is not possible, the collective interest should be given the greater priority.
- Decision-making processes will be transparent.

7 Developing the e-GIF

7.1 How to extend the e-GIF

The custodian and steward of the e-GIF encourage agencies to submit technical standards, especially schemas, that have been developed for specific agency business needs or for the needs of several agencies in a sector or area of business.

Inclusion in the framework ensures that such standards are widely recognised in the New Zealand public sector and can be applied, where appropriate, to meet business needs elsewhere in the sector.

The governance processes put in place for the e-GIF aim to balance the collective interest of government as a whole with the interests of individual agencies and their stakeholders. Where this is not possible, collective interest should be given the greater priority.

7.2 Submitting a new standard

The e-GIF is regularly reviewed and updated by issuing a revised version of this document. Extensions to the e-GIF can be suggested at any time, however. This should be done by first contacting e-gif@ssc.govt.nz.

Proposed extensions will be reviewed by working groups that advise the e-GIF custodian. The custodian makes recommendations to the e-GIF steward, via the e-GIF Management Committee.

Agencies that are required to adopt the e-GIF may appeal decisions to the Management Committee.

The standards-submission process, together with a template to propose a new standard, can be found at http://www.e.govt.nz/interoperability/faq.asp. Please note that the agency proposing the standard is expected to take a share in the development and governance of the standard.

7.3 Principles for developing the framework

As well as the principles outlined in this document, a number of guiding principles for the long-term development of the e-GIF are detailed in the Roadmap for the e-GIF.

7.4 Alignment with other framework initiatives

Open standards feature strongly in the e-GIF. OASIS, W3C, ISO and other standards organisations are developing standards with a global user base in mind.

The New Zealand e-GIF also draws from other jurisdictions, most notably the UK and Australia.

Agencies and service sectors are encouraged to draw from open standards to facilitate a greater level of uptake for bundled services in the future.

7.5 Issues under review

The 2005 e-GIF Review Group recommends the following strategies for further developing the e-GIF:

- **Extending the layer model** – The layer model categorises the technology standardised by the e-GIF structurally but not functionally. In practice, standards have a context. Some standards may only work in a particular situation, for a particular domain, depend on the use of other standards, or represent high-level aggregations of lower-level components. One possibility is to include additional columns in the table, such as "Applicable to", "Used by", "Used with", "Pre-requisites" and/or "Relies on". Another possibility is to create an additional category or layer for the emerging use of implementation profiles for XML-based standards.
- **Changing "R (Recommended)" to "E (Emerging)"** – There is some confusion about the word "recommended". For example, a new version of a product might be better, therefore recommended, but actually less interoperable until more agencies use it. Ultimately we would like to see the new version used, and therefore we recommend it when upgrading. Another ambiguity is that some may believe that if a standard is "adopted", it is *the* standard; and therefore, why would another be "recommended"? To address these concerns, another word such as "Emerging" might replace Recommended in future for this status level.
- **Adding a "Review Cycle" column** – Since standards proceed through a cycle of compliant statuses, a Review Cycle column could be added to the standards table to indicate how long each standard is in force and when it is up for review.
- **Continuous review cycles** – Since technology is continually changing, at an accelerating pace, for the e-GIF to remain relevant it should be updated continuously.
- **Using RFC 2119 –** To clarify the interpretation of key words related to the standards, consider using this RFC, which standardises use of the words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" when specifying requirement levels.

PART III: APPENDIXES

This part contains resources related to the e-GIF. It includes the following sections.

A. Abbreviations

ADL	Advanced Distributed Learning
AS2	Applicability Statement 2
ASCII	American Standard Code for Information Interchange
B2B	Business-to-business
BPEL4WS	Business Process Execution Language for Web Services
CSV	Comma Separated Values
CFL	Controlled Vocabulary or Code Lists
DOM	Document Object Model
DNS	Domain Name Server
DSML	Directory Services Markup Language
DSS	Digital Signature Services
DTD	Document Type Definition
ebXML (RIM, RS, MSG)	E-business XML (Registry Information Model, Registry Services, Messaging Services)
EDI	Electronic data exchange
EGU	The E-government Unit of the State Services Commission
ESA	Emergency Services in Government Administration
ESP	IP Encapsulation Security Protocol
FTP	File Transfer Protocol
GCSB	Government Communication Security Bureau
GIF	Graphical Interchange Format
GML	Geography Markup Language
HL7	Health Level 7
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol running over SSL
IP-SEC	IP Security Authentication Header
LDAP	Lightweight Directory Access Protocol
MIME, S/MIME	Multi-Purpose Internet Mail Extensions, Secure Multi-Purpose Internet Mail Extensions
NAT	Network Address Translation
NTPV	Network Time Protocol
NZGLS	New Zealand Government Locator Service
NSGMS	New Zealand Geospatial Metadata Standard

NZSIT	New Zealand Security of Information Technology
OASIS	Organization for the Advancement of Structured Information Standards
ODFOA	Open Document Format for Office Applications (OpenDocument)
PAS	Privacy, Authentication and Security
PKI	Public Key Infrastructure
PNG	Portable Network Graphic
RDF	Resource Description Framework
RSS	Rich Site Summary
SAML	Security Assertion Markup Language
SAX	Simple API for XML
SCORM	Shareable Content Object Reference Model
SCP	Session Control Protocol
SDMX	Statistical Data and Metadata Exchange
S.E.E.™ PKI	Secure Electronic Environment Public Key Infrastructure
S-HTTP	Secure HTTP
SIGS	Security in the Government Sector
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SSC EGU	State Services Commission E-government Unit
SSH	Secure Shell
SSL	Secure Sockets Layer
SVG	Scalar Vector Graphics
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
TNEF	Transport Neutral Encapsulation Formats
UBL	Universal Business Language
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol
UML	Unified Modelling Language
URN	Unique Resource Name
UTC (MSL)	Universal Time Clock (Measurement Standards Laboratory)
UTF	Unicode Transformation Fomat
VPN	Virtual Private Network
W3C	World Wide Web Consortium

WebDAV	World Wide Web Distributed Authoring and Versioning
WFS	Web Feature Server
WMS	Web Map Server
WSDL	Web Services Definition Language
WS-I	Web Services-Interoperability Organisation
xACML	Extensible Access Control Markup Language
xBRL	Extensible Business Reporting Language
xCIL	Extensible Customer Information Language
xCRL	Extensible Customer Relationships Language
XHTML	Extensible HyperText Markup Language
XMI	XML Metadata Interchange
XML	Extensible Markup Language
XML-DSig	XML Digital Signatures
XMPP	Extensible Messaging and Presence Protocol
xNAL	Extensible Name and Address Language
XSL	Extensible Stylesheet Language
XSLT	Extensible Stylesheet Language Transformations

B. History of the e-GIF

B.1 The UK e-GIF

The original version of the New Zealand e-GIF was based on work done by the Office of the UK e-Envoy in producing the UK e-GIF, which was first published in 2000. The UK e-GIF was reviewed by working groups comprising agency and vendor representatives during the latter part of 2001.

B.2 NZ e-GIF v1

Version 1 of the NZ e-GIF was published in May 2002 incorporating feedback from some 25 agencies. In June 2002 Cabinet agreed the NZ e-GIF would govern how public sector organisations are to achieve electronic interoperability of their information, technology and business.

B.2 Current NZ e-GIF

The current version of the e-GIF is available at http://www.e-gif.govt.nz. All major revisions to the e-GIF supersede earlier versions.

B.3 Change log

Version 3.0 (13 June 2005)

This is a substantial rewrite to make the e-GIF clearer and broader. In particular:

- Re-structured the document, separating Standards, Policy, and Appendixes.
- Added general information about e-government, interoperability, and the e-GIF.
- Clarified how to comply; included requirement for data-share agreements.
- Added agency and time limitations to exemption requirements.
- Revised layer model:
  - added Best Practice
  - separated out Web Services
  - changed "Architecture" to "Data Integration"
  - changed "E-government Component Architecture" to "E-government Services" and put in a separate section.
- Changed "categories" to "compliant status levels"; added new status classifications (F, U, R, A, D), diagram, and explanations.
- Added links to standards, procedures for submitting standards, applying for exemptions, the roadmap, and other resources on the internet.
- Re-structured standards table, added comments.

- Added, moved, removed, or revised the following standards:

Section	Component	Standards	Change
Network	Network Protocols (TCP/IP)	UDP	added
	File Transfer	WebDAV, SCP	added
	Registry Services (renamed, was "Registers")	DNS	added
		UDDI	moved to Web Services / Discovery
		ebXML	moved to Web Services / Messaging
	Time	NTPV, UTC (MSL)	added component
	Structured data description	RDF	moved to Business Services
	Metadata (Discovery)	NZGLS 2.0, NZGLS Thesauri	moved to Business Services
	Messaging Transport	HTTP 1.1	added component
	Messaging Formats	MIME	added component
Data Integration (renamed, was "Architecture")	Primary Character Set	ASCII	added
		Unicode	moved to omment:: an extension of ASCII
	Graphics File	GIF89a, JPG, PNG, SVG	moved to Access and Presentation / Website Presentation (comment)
	Mail Attachment	MIME	moved to Network / Messaging Formats
		S/MIME	moved to Security / Business Services
	Structured Web Document Language	HTML 4.01	renamed component, was "Hypertext"
	Data Transformation	XSLT	moved to Best Practice / XML Data Transformation
	Document Type Definition	DTD	added component
	Batch/Bulk Data	CSV	added component
	File Compression	GZIP	added
	File Archiving	TAR	added component
	Data Modelling	UML, XMI	moved to Best Practice
Web Services	(all components)	(all standards)	added section
Business Services	Metadata (Discovery)	RDF	moved from Network / Structured Data Description

Section	Component	Standards	Change
Business Services (cont.)	Presentation	GIF89a, JPG, PNG, SVG, PDF	moved to Access and Presentation / Website Presentation
	Namespace	URN	added component
	Structured data description	RDF	moved to Metatdata (Discovery) cvomponent
		XML 1.1	added
	Name and Address	xNAL v2	specified version
	Data Modelling	UML, XMI	moved to Best Practice
	Web Services (Description)	SOAP 1.2	moved to Web Services / Access
		WSDL 1.1	moved to Web Services / Description
	Processing (Structured Data)	SAX, DOM	renamed, was “Modelling (Structured Data)”: moved to Best Practice
	Additional Customer Information	xCIL, Data formats for identity records standard	added component
	Customer Relationship	xCRL	added component
	e-Learning	ADL, SCORM, and IMS	added component
	Business Reporting	xBRL	added component
	Directory Services	DSML	added component
	Statistical Data and Metadata	SDMX	added component
	Geospatial	NZGMS	added
	Registry Services (renamed, was “Registers”)	ebXML RIM and RS v2.1 & 3.0	specified versions
		UDDI	moved to Web Services / Discovery
	Content Syndication and Channel Feeds	RSS	renamed component, was “News Syndication”
	Instant Messaging	XMPP	added component
	Vice Over Internet Protocol	H.323V2, SIP	added component

Section	Component	Standards	Change
Access and Presentation	General Text and Graphics	HTML 4.01, GIF89a, JPG, PNG, SVG, PDF	moved to Website Presentation (comment)
	Website Presentation	NZ Govt Web Guidelines 2.1	added component
	Forms	xForms	added component
	Authentication Standards	Evidence of identity, Username / passwords, "Key type 2", Authentication key strengths, Trust levels for online transactions	spelled out separate standards
Security (re-sorted components by layer model)	Network	HTTPS, S-HTTP, TLS, IP-SEC, ESP	added
	Data Integration	XML – Enc	added
		XML – Dsig or OASIS DSS	added
	Web Services	SAML v2, Shared Logon assertion messaging standard	added
	Business Services	S/MIME v3	specified version
Best Practice	(all components)	(all standards)	added section
E-government services (renamed, was "E-government Component Architecture")	Autonomy		removed
	Shared Workspace		added
	Government Intranet		added
	SecureMail		added

Version 2.1 (14 May 2004)

- NZ xNAL schema added to Recommended to clarify the standard.

Version 2.0 (1 December 2003)

This is a substantial rewrite to clarify intent and make e-GIF more accessible. In particular:

- A new layer model was introduced and the old one removed.
- The old divisions of: Interconnection; Information Sharing and Exchange; Access; and Service delivery were removed. Standards were reclassified into: Network; Architecture; Business Services; and Access and Presentation.
- A list of e-Government components was added.
- The terms Standards and Guidelines were replaced with Mandatory and Recommended to clarify intent.

All standards have been reclassified in the move to version 2. In addition, the following standards have seen changes in status:

- Promote PNG (portable network graphics) to an option in the Mandatory class (others are GIF and JPG) due to maturity of standard.

- Correct XSL to XSLT under data transformation services.
- Add version number on ZIP compression standard – now ZIP 2.3.
- Add xNAL as Mandatory standard for Name and Address data transfers.
- Make SAX a Mandatory standard was a (guideline, now called Recommended) for modelling structured data.
- Add New Zealand Government RSS as a future standard for news syndication.
- Add a placeholder for authentication standards with a note to seek EGU advice.
- Updated reference to New Zealand Government Web Guidelines to current version (2.1).
- Add note about SecureMail as potential future government to citizen hardened email standard.
- Add lists of EGU components – available and under development.

Version 1.1 (3 July 2003)

- Add ESA as recommended standard.

Version 1.0 (13 June 2002)

Initial release.

C. References and background information

D.1 e-Government strategy

The e-government strategy is periodically reviewed and updated. The current version of the strategy can be found at http://www.e-government.govt.nz/programme/strategy.asp.

D.2 Policy framework for government-held information

All aspects of the Policy Framework for Government-held Information apply to data and information that is shared, exchanged, or otherwise used or managed under the specifications or coverage of the e-GIF. This requirement extends to the e-GIF itself.

D.3 Privacy Act 1993

The development and application of the e-GIF must comply with the Privacy Act.

D.4 Security in the Government Sector

The development and application of the e-GIF must comply with Security in the Government Sector.

D.5 Information Systems and Data Management Policies and Standards

While the e-GIF applies when agencies share information, technology and business processes, the Information Systems and Data Management Policies and Standards provide good-practice guidance for internal aspects of agency information and technology management:

- http://www.e-government.govt.nz/docs/data-management-policies/
- http://www.e-government.govt.nz/docs/is-policies-standards/
- http://www.e-government.govt.nz/docs/data-management-standards/

D. URLs referenced in this document

This document references several resources on the Internet, including:

- standards
- e-GIF documents
- other New Zealand Government documents
- other resources.

All links are spelled out (for hard copy) in the following tables.

E1 Standards

Standard	URL
AS2	http://www.ietf.org/internet-drafts/draft-ietf-ediint-as2-20.txt
ASCII	http://www.columbia.edu/kermit/ascii.html
Authentication	http://www.e-government.govt.nz/authentication/index.asp
BPEL4WS	http://www-128.ibm.com/developerworks/library/specification/ws-bpel/
CSV	http://www.answers.com/main/ntquery?method=4&dsid=1512&dekey=comma+delimited&gwp=8&curtab=1512_1
CVLs	http://www-128.ibm.com/developerworks/library/specification/ws-bpel/ (Discussion on standardising)
DNS	http://www.ietf.org/rfc/rfc1035.txt, http://www.cert.org/archive/pdf/dns.pdf (DNS Security)
DocBook	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=docbook
DOM	http://www.w3.org/DOM/
DRM	http://www.e.govt.nz/trusted/trusted.asp (October 2004 paper on Trusted Computing)
DSML	http://www.oasis-open.org/specs/index.php#dsmlv2
DTD	http://www.w3.org/TR/REC-html40/intro/sgmltut.html http://www.w3schools.com/dtd/default.asp (W3School's DTD Tutorial)
ebXML	http://www.ebxml.org/
ebXML MSG	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-msg
ebXML RIM and RS V2.1 & v3.0	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=regrep
ESA	http://www.linz.govt.nz/rcs/linz/pub/web/root/core/Topography/ProjectsAndProgrammes/emergencyservices/index.jsp
ESP	http://www.ietf.org/rfc/rfc2406.txt
FIPS 140-1 140-2	http://csrc.nist.gov/cryptval/140-1/1401val.htm, http://www.nist.gov/ (NIST)

Standard	URL
FTP	http://www.ietf.org/rfc/rfc0959.txt, http://www.ietf.org/rfc/rfc2228.txt (FTP security extensions), http://www.ietf.org/rfc/rfc1579.txt (FTP via Port 80)
GCSB NZSITs	http://www.gcsb.govt.nz/nzsit/index.htm
GIF 89a	http://www.w3.org/Graphics/GIF/spec-gif89a.txt
GML	http://www.opengis.org/techno/implementation.htm
GZIP	http://www.gzip.org/
H.323V2	http://www.openh323.org/, http://computing-dictionary.thefreedictionary.com/codec (Codec)
HL7	http://www.hl7.org/
HTML 4.01	http://www.w3.org/TR/html401/
HTTP 1.1	http://www.ietf.org/rfc/rfc2616.txt
HTTPS	http://www.ietf.org/rfc/rfc2818.txt
IP-SEC	http://www.ietf.org/rfc/rfc2402.txt, http://www.ietf.org/rfc/rfc2404.txt (IP Security Authentication Header)
IPv4	http://www.ietf.org/rfc/rfc0791.txt
IPv6	http://www.itef.org/rfc/rfc2460.txt
JPG	http://www.ietf.org/rfc/rfc2435.txt
LDAP v3	http://www.ietf.org/rfc/rfc1777.txt
Metalogue	http://www.e-government.govt.nz/docs/muggles-200405/chapter15.html
MIME	http://www.ietf.org/rfc/rfc2049.txt
NTPv4	http://www.ntp.org/
NZGLS 2.0	http://www.e-government.govt.nz/nzgls/standard/
NZGLS Thesauri	http://www.e-government.govt.nz/nzgls/thesauri/downloads.asp
NZGMS	http://www.e.govt.nz/interoperability/nzgms.asp
NZ Govt Web Guidelines 2.1	http://www.e-government.govt.nz/docs/web-guidelines-2-1/index.html
OASIS DSS	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss
ODFOA 1.0	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office
OpenSAML	http://www.opensaml.org/
PAL project	http://www.pco.parliament.govt.nz/pal/
PAS	http://www.standards.com.au/catalogue/script/Details.asp?DocN=AS401174312067 (AS/NZS ISO/IEC 17799:2001)

Standard	URL
PDF	http://www.adobe.com/products/acrobat/adobepdf.html
PNG	http://www.libpng.org/pub/png/
Portal News Feed	http://www.e-government.govt.nz/docs/rss-v-1-0-final/index.html
RDF	http://www.w3.org/RDF/
RSS	http://web.resource.org/rss/1.0/
SAML	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
SAX	http://www.w3.org/DOM/
SCP	http://www.w3.org/Protocols/HTTP-NG/http-ng-scp.html
SDMX	http://www.sdmx.org/
SecureMail	http://www.e.govt.nz/securemail/index.asp
SEE MAIL	http://www.see.govt.nz/mail/
SEE Mail	http://www.e-government.govt.nz/see/mail/index.asp
SEE PKI	http://www.see.govt.nz/pki/ http://www.e-government.govt.nz/see (SEE)
Shared Workspace	http://www.e-government.govt.nz/workspace/index.asp
S-HTTP	http://www.terisa.com/shttp/current.txt
SIGS	http://www.security.govt.nz/sigs/sigs.pdf, http://www.iso17799software.com/ (ISO 17799)
SIP	http://www.ietf.org/html.charters/sip-charter.html, http://computing-dictionary.thefreedictionary.com/codec (Codec)
S/MIME V3	http://www.ietf.org/rfc/rfc2633.txt
SMTP	http://www.ietf.org/rfc/rfc2821.txt, http://www.cert.org/tech_tips/email_spoofing.html (spoofing)
SOAP 1.2	http://www.w3.org/TR/2001/WD-soap12-20010709/
SSL v3	http://www.netscape.com/eng/ssl3/draft302.txt
SVG	http://www.w3.org/Graphics/SVG/Overview.htm8
TAR	http://www.gnu.org/software/tar/tar.html
TCP	http://www.ietf.org/rfc/rfc793.txt
TLS	http://www.ietf.org/rfc/rfc2246.txt
Trusted Computing	http://www.e.govt.nz/docs/trust-security-2004/index.html (Discussion paper on Trust and Security on the Internet), http://www.e.govt.nz/trusted/index.asp (EGU Report on Trust & Security)
UBL	http://www.oasis-open.org/committees/sc_home.php?wg_abbrev=ubl-ndrsc

Standard	URL
UDDI	http://www.uddi.org/specification.html, http://www.w3.org/TR/2001/NOTE-wsdl-20010315 (WSDL)
UDP	http://www.faqs.org/rfcs/rfc768.html, http://www.networksorcery.com/enp/protocol/udp.htm
UML	http://www.omg.org/technology/uml/index.htm
Unicode	http://www.unicode.org/
URN	http://www.e.govt.nz/interoperability/namespaces.asp, http://www.ietf.org/internet-drafts/draft-hendrikx-wallis-urn-nzl-00.txt (Internet Draft)
UTC (MSL)	http://www.irl.cri.nz/msl/services/time/, http://www.unicode.org/ (Unicode Transformation Fomat)
UTF – 8 bit encoded	http://www.ietf.org/rfc/rfc2279.txt
W3C schema definitions	http://www.w3.org/TR/xmlschema-1/
WebDAV	http://www.ietf.org/rfc/rfc2518.txt
WFS	http://www.opengeospatial.org/specs/
Win SCP	http://winscp.net/eng/index.php
Wireless standard	http://www.cnp-wireless.com/ArticleArchive/Wireless%20Telecom/2002Q3-SMSInterworking.htm (Cellular Networking Perspectives LTD article on SMS Interoperability)
WMS	http://www.opengis.org/techno/implementation.htm
WordML	http://www.xmlw.ie/aboutxml/wordml.htm
WS-I Basic Profile 1.1	http://www.ws-i.org/profiles/BasicProfile-1.1-2004-08-24.html
WSS-I Basic Profile 1.0	http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0-2004-05-12.html
WS - Security	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
WSDL 1.1	http://www.w3.org/TR/2001/NOTE-wsdl-20010315
WSE2 0	http://www.microsoft.com/downloads/details.aspx?FamilyId=FC5F06C5-821F-41D3-A4FE-6C7B56423841&displaylang=en
xACML V2.0	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml
xBRL	http://www.xbrl.org/Home/
xCIL	http://www.oasis-open.org/committees/ciq/ciq.html#7
xCRL	http://www.oasis-open.org/committees/ciq/ciq.html#8
xForms	http://www.w3.org/TR/2003/REC-xforms-20031014/
XMI	http://www.omg.org/technology/documents/formal/xmi.htm
XML 1.0	http://www.w3.org/TR/REC-xml
XML 1.1	http://www.w3.org/TR/2002/WD-xml11-20020425/

Standard	URL
XML-DSig	http://www.w3.org/TR/2002/REC-xmldsig-core-20020212
XML encryption	http://www.w3.org/TR/xmlenc-core/
XMPP	http://www.ietf.org/rfc/rfc3920.txt
xNAL (nz) schema	http://www.e.govt.nz/interoperability/xnal/index.asp
xNALV2	http://www.oasis-open.org/committees/ciq/ciq.html#4
XSL	http://www.w3.org/Style/XSL/
XSLT	http://www.w3.org/Style/XSL/
ZIP 2.3	http://www.info-zip.org/

E2 e-GIF documents

Document	URL
December 2001 New Zealand E-government Strategy	http://www.e-government.govt.nz/docs/e-gov-strategy-dec-01/
June 2003 E-government Strategy Update	http://www.e-govt.govt.nz/docs/e-gov-strategy-june-2003/
Current version of the e-GIF	http://www.e-gif.govt.nz.
Roadmap for the e-GIF	http://www.e-government.govt.nz/docs/e-gif-roadmap/
Frequently Asked Questions and answers about e-GIF	http://www.e-govt.govt.nz/interoperability/faq.asp

E3 Other New Zealand Government documents

Document	URL
New Zealand Government Data Management Standards	http://www.e-government.govt.nz/docs/data-management-standards/
New Zealand Government Data Management Policies	http://www.e-government.govt.nz/docs/data-management-policies/
New Zealand Government Information Systems Policies and Standards	http://www.e-government.govt.nz/docs/is-policies-standards/

Document	URL
NZ Govt Web Guidelines 2.1	http://www.e-government.govt.nz/docs/web-guidelines-2-1/index.html
Guidelines for Managing and Monitoring Major IT Projects	http://www.ssc.govt.nz/ITguidelines
Policy framework for government-held information	http://www.ssc.govt.nz/documents/policy_framework_for_Government_.htm
Privacy Act	http://www.privacy.org.nz/comply/comptop.html
Security in the Government Sector	http://www.security.govt.nz/sigs/
October 2004 paper on Trusted Computing	http://www.e.govt.nz/trusted/trusted.asp
EGU Report on Trust & Security	http://www.e.govt.nz/trusted/index.asp

E4 Other resources

Document	URL
Office of the UK e-Envoy	http://www.e-envoy.gov.uk/
UK Technical Standards catalogue Version 6.2	http://www.govtalk.gov.uk/documents/TSCv6.2_2005_4_29.pdf
Organization for the Advancement of Structured Information Standards (OASIS)	http://www.oasis-open.org/
International Organization for Standardization (ISO)	http://www.iso.org/
World Wide Web Consortium (W3C)	http://www.w3c.org/
RFC 2119 (Key words for use in RFCs to Indicate Requirement Levels)	http://www.faqs.org/rfcs/rfc2119.html