New Zealand E-government

Interoperability Framework

(NZ e-GIF)

Version 3.0

INTRODUCTION

March 2006

State Services Commission

1   Foreword

The E-government Interoperability Framework (e-GIF) was first issued in February 2002. This version (v3.0) is the seventh edition to be published.

In the three and a half years since the initial launch, we have seen tremendous change in New Zealand, both in the public sector and in wider society. Technology continues to advance and government agencies' business needs keep evolving in response to the changes in technology and society. The challenges and opportunities these changes present demand innovative and collaborative solutions from government agencies.

Since 2002, the e-GIF has proved to be a significant tool for enabling agencies to work together and for all-of-government initiatives. By promoting collaboration and the efficient use of resources, the e-GIF contributes to the State Services Development Goals of Networked, Coordinated and Accessible State Services.

The e-GIF has formed the foundation of a number of important e-government initiatives.   The framework has helped collaboration between government agencies, resulting in more integrated services for New Zealanders. For example:

- Customers can now register for a company IRD number online when they incorporate a company. This service eliminates the need for new companies to deal with the Companies Office and Inland Revenue separately. It makes the registration process faster by eliminating duplication of information between agencies and the need to provide paper-based IRD number applications.

- SEEMail, the Secure Electronic Environment Mail standard, helps the secure exchange of email and attachments using the Internet. It is now used by 51 government agencies.

- www.govt.nz, the all-of-government web portal, uses e-GIF standards to collect information about government services from a wide range of government agencies. It provides an online single point of access for New Zealanders.

These online services and resources have been made possible by the e-GIF, and the people from across government who have worked together on this version, and all the earlier versions, of the framework.

Over the coming years standards will continue to be added to the e-GIF, and the framework will grow to accommodate them.

We welcome the publication of this latest version and acknowledge the collaborative effort that has achieved this. We are also confident this valuable resource will continue to provide the foundation for future e-government initiatives across the State Services.

Laurence Millar

Deputy Commissioner, Information and Communication Technologies Branch

Warren Tucker

Chairperson, e-GIF Management Committee

About the e-GIF documents

The E-government Interoperability Framework (e-GIF) Version 3.0, consists of three documents:

- Part 1: Standards

- Part 2: Policy

- Part 3: Resources

Below are short descriptions of each document and its intended audience.

Part 1: Standards

Part 1 focuses on the standards that make up the e-GIF. The intended audience for this section includes:

- State sector information technology (IT) strategists

- technical analysts

- programme and project managers

- anyone planning services requiring interoperability.

Part 1 includes the following sections:

- **How to read the standards:** Description of the layer model used to categorise the standards, what the status levels for each standard mean, links to related documentation, and changes from the last e-GIF.

- **e-GIF standards:** The standards listed by category.

- **E-government services:** Services that are part of the e-government programme, fully support interoperability, and are freely available to public sector agencies.

Part 2: Policy

Part 2 outlines the policy behind the e-GIF and its development. The intended audience for this section includes:

- policy analysts

- advisors

- business analysts

- anyone involved with interoperability strategy and projects.

Part 2 includes the following sections:

- **What is the e-GIF?** Short descriptions of e-government, interoperability, and the e-GIF, how the e-GIF will benefit New Zealand, and how the e-GIF is maintained.

- **Who must comply and when?** Who must comply with the e-GIF, how to transition to e-GIF compliance, exemptions and special provisions.

- **Principles**: Short descriptions of anticipated outcomes of the e-GIF, requirements for project and operational management, and governance principles.

- **Developing the e-GIF:** 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.

Part 3: Resources

Part 3 contains resources related to the e-GIF. The intended audience for this section is all readers of the e-GIF.

Part 3 includes the following sections:

- **History of the e-GIF:** Review of stages in the e-GIF's development, including a Change Log.

- **References and background information:** Descriptions and links to further information related to the e-GIF.

- **URLs referred to in the e-GIF:** Full URLs for all hyperlinks in the e-GIF documents.

- **Abbreviations:** Definitions of abbreviations and acronyms used in the e-GIF.

New Zealand E-government

Interoperability Framework

(NZ e-GIF)

Version 3.0

PART 1 – STANDARDS

March 2006

State Services Commission

About this document

This document focuses on the standards that make up the e-GIF. The intended audience for this Standards section includes:

- State sector information technology (IT) strategists

- technical analysts

- programme and project managers

- anyone planning services requiring interoperability.

It includes the following sections:

- How to read the standards: Description of the layer model used to categorise the standards, what the status levels for each standard mean, links to related documentation, and changes from the last e-GIF.

- E-GIF standards: The standards listed by category.

- E-government services: Services that are part of the e-government programme, fully support interoperability, and are freely available to public sector agencies.

1 How to read the standards

The e-GIF standards[1] are categorised using a "layer model".

Each protocol, standard or convention (de facto standard) is listed with a version number, where applicable, a status level and any relevant comments. Note that in computing, protocols are generally used to define real-time communications behaviour, while standards are used to govern the structure of information committed to long-term storage.

This section explains how to read the list of standards.

1.1 Layer model

Layer models are widely used to classify functions within IT systems. They are used 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

---

1 In the e-GIF, protocols and standards are both referred to as "standards". Note that protocols are sometimes distinguished as a specific type of standard — see http://en.wikipedia.org/wiki/Protocol_%28computing%29 and http://en.wikipedia.org/wiki/Communications_protocol.

The four basic structural components, or 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 that security 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:** This is a 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 which the ICT Branch of the State Services Commission makes available for public sector agencies to use. (See Section 3 E-government Services).

- **Web Services:** Web Services connect services together. They are an emerging set of standardised applications to connect and integrate web-based applications over the Internet. Using Best Practice implementations, agencies can agree a common approach to interoperable service delivery to customers.

Underpinning all these layers are:

- **Management:** See Part 2, Section 1.4 Managing the e-GIF.

- **Governance**: See Part 2, Section 1.4 Managing the e-GIF and Section 3.4 Governance Principles. An e-GIF Governance Overview paper is also available from the ICT Branch of the State Services Commission. Please email e-GIF@ssc.govt.nz.

1.2   Compliance status levels

The status level of an e-GIF standard shows 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 the following levels: **Adopted**, **Recommended**, **Under Development**, and **Future Consideration**. The revised status levels broadly align with those used in the UK e-GIF[2]. The requirement for an additional category, **Deprecated**, became 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, it gives it an appropriate status. When the standard matures, the Committee can consider recommendations to change its status.

---

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

1.3   Current e-GIF compliance status levels

The current e-GIF compliance status levels for standards are illustrated and described below.
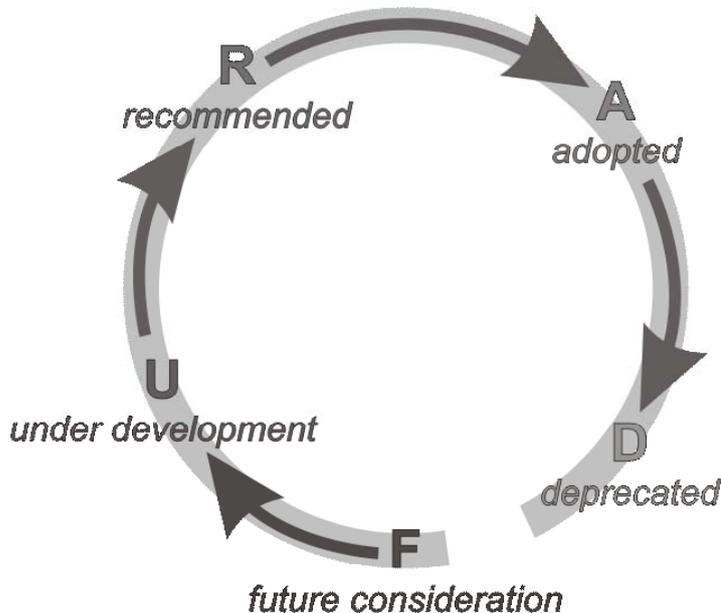
Figure 2: e-GIF Compliance Status Levels

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

- **Future Consideration (F):** Not yet reviewed, customised, or having any successful, documented implementation in the New Zealand government; yet probably necessary for public sector IT systems. Included mainly to introduce these standards 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, e.g. 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

  - scaleable

  - 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 and 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.

  Note: The main difference between Recommended and Adopted is the maturity, which can be equated with well-understood software version models.

  - A standard that is Adopted has widespread use and industry acceptance. It is the default standard in use, and is not expected to become Deprecated within 12 months. There is no immediate onus on existing interoperability agreements to migrate to the newer Recommended standard.

  - Where a standard is Recommended, there is growing industry adoption. New interoperability initiatives are more likely to use this standard.

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

1.4   Choosing between standards

Given the need to maintain the e-GIF so that it keeps pace with changing technology, multiple standards may be available for a 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 agencies whose functions and services relate to your own (your likely interoperability partners)

- then, together, agree a standard, considering the compliant status levels:

  - Use **Recommended (R)** standards if you can; they are generally newer and less subject to obsolescence than **Adopted (A)** standards.

  - If you cannot, or do not wish to, use **R**, use **A** if you can. An **A** standard is the default; but if an **R** standard also exists, you are encouraged to use it.

  - If you cannot use **R** or **A** standards, use any applicable **Future Consideration (F)** or **Under Development (U)** standards. Notify the ICT Branch of the State Services Commission for Working Group 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 ICT Branch for Working Group information.

  - Avoid new use of **Deprecated (D)** standards.

Note 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 they will be taking part in its development.

1.5   Links

Standards included in the e-GIF that are blue and underlined have links to an RFC or other resources on the Internet, which explain them more fully. If you are using a hard copy version of this document, see Part 3, Section 2 URLs referred to in the e-GIF.

1.6   Comments

The comments in the list of standards provide 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.

1.7   Changes from previous version

The following elements in the list of standards are new to e-GIF v3.0:

- **Status levels:**   Version 2.1 standards were either Mandatory or Recommended; this version uses the scheme described in Section 1.3.

- **Standards listing:** The list of standards now notes the status level of each standard and includes relevant comments.

- **Web Services section:** Section 2.6.4 includes standards specifically related to web services implementation that do not strictly fit into the layer model.

- **Best Practice section:** Section 2.7 includes standards that do not strictly fit into the layer model but rather apply only in a particular context.

- **Added, moved, removed, revised standards:**   See Part 3, Section 1.4 Change Log . Note there are a number of new standards in the e-GIF v3.0; many of these were considered necessary to implement existing e-GIF standards.

2   e-GIF standards

This section sets out the current and emerging standards required for e-GIF compliance and to facilitate interoperability.

- **See Part 3, Section 3 Abbreviations** for definitions of abbreviations and acronyms used in this section.

- **See Part 3, Section 1.4 Change Log** for a list of standards that are new, moved, removed, or changed in this version.

- **Links** in the list of standards to online resources, usually the standards themselves, explain more fully what each standard covers; see also Part 3, Section 2 URLs referred to in the e-GIF.

- Note that **multiple standards** may exist in any category; see Section 1.4 Choosing between standards.

2.1 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.

Network protocols (TCP/IP)						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
TCP Transmission Control Protocol					•	
UDP User Datagram Protocol	A lower service level alternative to TCP, offers minimal transport service for applications using multicast/ broadcast delivery, DNS, routing information, and network management. Omission from previous version.				•	
IP v4 Internet Protocol Version 4	Plan for migration to IP v6. New hardware should support IP v4 as well as IP v6.				•	
IP v6 Internet Protocol Version 6	When implementing IP v6, configure routers to "ghost" IP v4.			•		

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = recommended; **A** = adopted; **D** = deprecated.

Directory protocols						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
LDAP v3 Lightweight Directory Access Protocol Version 3.	For access to directory services.			•		

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = recommended; **A** = adopted; **D** = deprecated.

File transfer protocols						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
FTP File Transfer Protocol	Use restart and recovery. Also FTP security extensions and FTP via Port 80 where applicable.				•	
HTTP v1.1 HyperText Transfer Protocol Version 1.1	Application level protocol. See Security layer for secure HTTP (HTTPS) and TLS usage.				•	
WebDAV World Wide Web Distributed Authoring and Versioning	A set of extensions to HTTP v1.1 that allows users to collaboratively edit and manage files remotely but avoids access problems with NAT firewalls.	•				
SCP Session Control Protocol	A simple protocol, which lets a server and client, have multiple conversations over a single TCP connection. The main function of SCP is to define a file transfer method that supports the transfer of files between a local and a remote computer. It uses Secure Shell (SSH) and supports Secure FTP.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = recommended; **A** = adopted; **D** = deprecated.

Mail transfer protocols						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
SMTP Simple Mail Transfer Protocol	Host-to-host protocol. Beware of spoofing of email addresses. SMTP-TLS is used to protect mail headers.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = recommended; **A** = adopted; **D** = deprecated.

Registry Services						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
DNS Domain Name Server	Use DNS for Internet/Intranet domain to IP address resolution. DNS Security is critical. Omission from previous version.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = recommended; **A** = adopted; **D** = deprecated.

Time protocols						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
NTP v4 Network Time Protocol Version 4	De facto standard proposed for use in an all-of-government time standard. Best practice guidelines are being developed.		•			
UTC (MSL) Universal Time Clock	De facto standard (accessed from Industrial Research	•				

Time protocols						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
(Measurement Standards Laboratory)	Limited, MSL); proposed for use in an all-of-government time standard. Best practice guidelines are being developed.					

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = recommended; **A** = adopted; **D** = deprecated.

Messaging transport						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
HTTP v1.1 HyperText Transfer Protocol Version 1.1	See File transfer and Security layer.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Messaging formats						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
MIME Multi-Purpose Internet Mail Extension	See also S/MIME and Security layer for secure mail attachments. Do not use Transport Neutral Encapsulation Formats (TNEF) for headers.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

2.2 Data Integration layer

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

Primary character set						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
ASCII American Standard Code for Information Exchange	Minimum set of characters for data interchange. Omission from previous version.				•	
UTF 8 bit encoded					•	
Unicode Transformation Fomat An extension of ASCII					•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; D = deprecated.

Structured web document language						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
HTML v4.01 HyperText Markup Language Version 4.01	For web content. See Web Guidelines Version 2.1.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Schema definition languages						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
XML v1.0 Extensible Markup Language Version 1.0	Meta-language to create tags to define, transit, validate, and interpret data.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Document type definition						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
DTD Document Type Definition	Describes multiple elements and attributes for XML; see W3School's DTD Tutorial.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Structured data						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
XML v1.0 Extensible Markup Language Version 1.0	Preferred option for structured data transport.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Batch/bulk data						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
CSV Comma-Separated Values	XML 1.0 is strongly preferred for structured data transport. Parties must agree file header records before exchange. Omission from previous version.					•

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

File compression						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
ZIP v2.3 ZIP Version 2.3	Other products using the compression algorithm LZH are also acceptable, subject to the agreement of the exchanging parties.				•	
GZIP GNU Zip	Not compatible with ZIP. Omission from previous version.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

File archiving						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
TAR Tape Archiver	Omission from previous version.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

2.3 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.

Metadata (Discovery)						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
NZGLS v2.0 New Zealand Government Locator Service Version 2.0					•	
NZGLS Thesauri New Zealand Government Locator Service Thesauri					•	
RDF Resource Description Framework	An XML file format to describe metadata. RDF is used by RSS1.0 (see below).				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Namespace						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
W3C schema definitions World Wide Web Consortium Schema Definitions	Use when other schemas customised for use by government agencies are not specifically identified (e.g. NZGMS, xNAL (nz), NZGLS).				•	
OIDS Schema Object Identifiers	The ICT Branch of the State Services Commission maintains 2.16.544.101 as the Government OID Arc.			•		

Namespace						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
URN Uniform Resource Name	Working Group to be led by ICT Branch of the State Services Commission. See also Internet Draft.		•			

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Schemas						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
W3C schema definitions World Wide Web Consortium Schema Definitions	Use when other schemas customised for use by government agencies are not specifically identified (e.g. NZGMS, xNAL (nz), NZGLS).				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Structured data description						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
XML v1.1 Extensible Markup Language Version 1.1	Erratum in previous version. (Note: "Structured data" refers to XML Version 1.0.)				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Name and address						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
xNAL v2 Extensible Name and Address Language Version 2	xNAL (OASIS) v3 being drafted; will be incorporated into e-GIF following a successful pilot.				•	
xNAL (nz) schema Extensible Name and Address Language (New Zealand)	Agency User Group led by ICT Branch of the State Services Commission; xNAL (nz) will ultimately be replaced by xNAL (OASIS) v3.			•		

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Additional customer information						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
Data formats for identity records standard	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.		•			
xCIL Extensible Customer Information Language	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.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Customer relationship						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
xCRL Extensible Customer Relationships Language	Part of the xCIL and xNAL family of standards specifying formats for relationships between customers.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

E-learning						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
ADL, SCORM, and IMS Advanced Distributed Learning, Shareable Content Object Reference Model, and Instructional Management System	Specifications currently being considered by the E-learning Working Group.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Business reporting						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
xBRL Extensible Business Reporting Language	Working Group underway, led by Inland Revenue.		•			

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Directory services						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
DSML Directory Services Markup Language		•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Statistical data and metadata						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
SDMX Statistical Data and Metadata Exchange	Statistics New Zealand leads this standard.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Geospatial						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
GML Geography Markup Language	Land Information New Zealand leads this standard.				•	
WFS Web Feature Server	Land Information New Zealand leads this standard.				•	
WMS Web Map Server	Land Information New Zealand leads this standard.				•	
ESA Emergency Services in Government Administration	Land Information New Zealand leads this standard.			•		
NZGMS New Zealand Geospatial Metadata Standard	Schema for identifying geospatial metadata. Land Information New Zealand leads this standard.			•		

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Registry services						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
ebXML RIM and RS v2.1 E-business Extensible Markup Language, Registry Information Model, and Registry Services Version 2.1	Open standard application for Registry Information and Records Services in an e-business context, as an alternative to Web Services.				•	
ebXML RIM and RS v3.0 E-business Extensible Markup Language, Registry Information Model, and Registry Services Version 3.0	Open standard application for Registry Information and Records Services in an e-business context, as an alternative to Web Services.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Content syndication and channel feeds						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
RSS Really Simple Syndication	Note that this standard is required for agencies using the government portal news service, E-government Shared Services.			•		

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Instant messaging						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
XMPP Extensible Messaging and Presence Protocol	XML protocol for real-time messaging. Taken from UK Technical Standards Catalogue Version 6.2.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Voice Over Internet Protocol (VOIP)						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
SIP Session Initiation Protocol	A protocol for initiating, modifying, and terminating an interactive user session that involves multimedia elements such as video, voice and instant messaging. Has greater take-up than H.323. Taken from UK Technical Standards Catalogue Version 6.2. Codec required.	•				
RTP Real-time Transport Protocol	Defines a standardised packet format for delivering audio and video over the Internet and is frequently used in conjunction with RTSP, H.323 or SIP.	•				
H.323 v2 H.323 Version 2	An umbrella recommendation from the ITU-T, which defines the protocols to provide audiovisual communication sessions on any packet network. Taken from UK Technical Standards Catalogue Version 6.2.	•				

Voice Over Internet Protocol (VOIP)						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
	Codec required.					
G.711	An ITU-T standard for audio companding; primarily used in telephony.	•				
G.729	An audio codec for voice that compresses voice audio in chunks of 10 milliseconds; is mostly used in VOIP applications for its low bandwidth requirement.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

2.4 Access and Presentation layer

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

Website presentation						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
NZ Govt Web Guidelines Version 2.1	See Web Guidelines v2.1 for use of: HTML 4.01, XHTML, GIF 89a, JPG, PNG, SVG, and PDF. Proposed change to Adopted status in 2006.			•		

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Web design and maintenance						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
NZ Govt Web Guidelines Version 2.1	See Web Guidelines v2.1 for use of: HTML 4.01, XHTML, GIF 89a, JPG, PNG, SVG, and PDF. Proposed change to Adopted status in 2006.			•		

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Forms						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
xForms	Open standard for use of XML forms on web pages, to replace HTML forms.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Authentication standards						
Note: Agencies wishing to implement any new systems where authentication of individuals or businesses is necessary must contact the ICT Branch of the State Services Commission for advice.						

Standard	Comments	Status level				
		F	**U**	**R**	**A**	**D**
Evidence of identity standard	Specifies a business process for establishing the identity of government agency customers.		•			
Username / passwords standard	Specifies use of username/passwords for online authentication.		•			
"Key type 2" standard	Specifies use of an as yet undefined key type for online authentication.		•			
Authentication key strengths standard	Specifies and populates a model for comparing the relative strengths of authentication keys.		•			
Trust levels for online transactions standard	Maps online transactions to authentication key strengths and evidence-of-identity confidence levels.		•			

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

2.5   Web Services layer

Web Services is 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 implementing web services across government.

The following standards apply where systems use web services architecture.

Discovery						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
UDDI v3 Universal Description, Discovery and Integration Version 3	An open standard for describing, publishing, and discovering network-based software components.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated.

Description						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
WSDL v1.1 Web Services Description Language Version 1.1	Specifies the location of the service and the operations, or methods, the service exposes.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

Access						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
SOAP v1.1 Simple Object Access Protocol Version 1.1	For Web Services Transport. E-GIF v3.0 recommends SOAP v1.2, but adopts SOAP v1.1 because of feedback from agencies that this is the version currently supported in many common development products.				•	
SOAP v1.2 Simple Object Access Protocol Version 1.2	Previous versions of the e-GIF adopted SOAP v1.2. E-GIF v3.0 recommends SOAP v1.2, but adopts SOAP v1.1 because of feedback from agencies that this is the version currently supported in many common development products.			•		

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

Messaging						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
ebXML MSG E-Business Extensible Markup Language Messaging Services	Also known as ebMS.	•				
AS2 Applicability Statement 2	A lightweight, open messaging transport for B2B messaging services. Comparable with ebXML MSG/ebMS.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

<table>
<tr><th colspan="7" align="center">Security</th></tr>
<tr><th rowspan="2">Standard</th><th rowspan="2">Comments</th><th colspan="5" align="center">Status level</th></tr>
<tr><th>F</th><th>U</th><th>R</th><th>A</th><th>D</th></tr>
<tr><td>WSS
Web Services Security</td><td>Security standard under development by OASIS.</td><td>•</td><td></td><td></td><td></td><td></td></tr>
<tr><td>SAML v2.0
Security Assertion Markup Language Version 2.0</td><td>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 Access and Presentation layer. OpenSAML is an implementation of SAML</td><td>•</td><td></td><td></td><td></td><td></td></tr>
<tr><td>xACML v2.0
Extensible Access Control Markup Language Version 2.0</td><td>XML Schema for creating policies and automating their use to control access to disparate devices and applications on a network.</td><td>•</td><td></td><td></td><td></td><td></td></tr>
</table>

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

<table>
<tr><th colspan="7" align="center">Compliance</th></tr>
<tr><th rowspan="2">Standard</th><th rowspan="2">Comments</th><th colspan="5" align="center">Status level</th></tr>
<tr><th>F</th><th>U</th><th>R</th><th>A</th><th>D</th></tr>
<tr><td>WS-I Basic Profile v1.1
Web Services – Interoperability Organisation Basic Profile Version 1.1.</td><td>Profiles provide implementation guidelines for how related web services specifications should be used together for best interoperability. To date, WS-I has finalised the Basic Profile, Attachments Profile and Simple SOAP Binding Profile.</td><td>•</td><td></td><td></td><td></td><td></td></tr>
<tr><td>WSS-I Basic Profile v1.0</td><td>Draft 1.0 Basic Security</td><td>•</td><td></td><td></td><td></td><td></td></tr>
</table>

Compliance						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
Web Services Security - Interoperability Organisation Basic Profile Version 1.0.	Profile accepted by OASIS.					

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

2.6   Security layer

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

- **Confidentiality:** Ensuring information is accessible only to those authorised to have access.

- **Integrity[3]:** Safeguarding the accuracy and completeness of information and processing methods.

- **Availability:** Ensuring authorised users have access to information and associated assets when required.

- **Accountability:** A system's ability to keep track of who or what has accessed data, conducted transactions, or made changes to the system[4].

Agencies are encouraged to consider the security implications of interoperability projects using these contexts, and apply the appropriate policies and standards. The following list 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.

Policy						
Standard	**Comments**	**Status level**				
		F	U	R	A	D
GCSB NZSITs Government Communications Security Bureau New Zealand Security of Information Technology Publications	Please note 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.				•	

---

3   Note: "Integrity" here does not refer to "data integrity", which is beyond the scope of the e-GIF. These standards are responsible for the integrity of the transport but not necessarily the integrity of the data.

4 Sourced from ISO17799: IT - Code of Practice for Information Security Management.

Policy						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
SIGS Security in the Government Sector	A manual of policies, principles and procedures mandated by Cabinet in 2001, largely drawn from ISO 17799. Page 8-20, paragraph 10 of SIGS requires use of an IS framework following ISO 17799 for all systems processing classified, including IN-CONFIDENCE, information or hosting government services. Individual security counter-measures defined in ISO17799 should be considered, but are not mandated.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

Network						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
HTTPS HyperText Transfer Protocol running over SSL	See SSL v3 below. Omission from previous version.				•	
SSL v3 Secure Sockets Layer Version 3	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.				•	
Ipsec Internet Protocol Security	Authentication header standard taken from NZSIT/SIGS. Omission from previous version.				•	
ESP IP Encapsulation Security Protocol for VPN	Requirements taken from NZSIT/SIGS. Omission from previous version.				•	
S-HTTP Secure HyperText Transfer Protocol	For individual messages, created by SSL running under HTTP.	•				
TLS Transport Layer Security	RFC 2616 upgrade mechanism in HTTP 1.1; initiate Transport Layer Security over an existing TCP connection. Does not yet interoperate with SSL v3.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

Data integration						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
XML – Enc XML-Encryption syntax and processing	Taken from UK Technical Standards Catalogue Version 6.2.	•				
XML - DSig or **OASIS DSS**	XML-Digital signature – syntax and processing as defined by W3C, used in SAML implementations. OASIS Digital Signature Services – developing an alternative implementation.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

Web services						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
SAML v2.0 Security Assertion Markup Language Version 2.0	**Comments** A subset of SAML v1.1, elements are Under Development as part of the All-of-government Authentication project. See Access and resentation layer	•				
Security Assertion Messaging standard	All-of-government Authentication project standard Under Development. Expected to specify four specific messages from SAML for communicating authentication assertions.		•			

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

Business services						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
SEE PKI Secure Electronic Environment Public Key Infrastructure	For agencies using the Secure Electronic Environment (SEE) e-government component. See Section 3 E-government Services for more details.			•		
SEEMail Secure Electronic Environment Mail	A combination of procedures and standards already listed in the e-GIF, required to use the e-government component SEEMail service. See Section 3 E-government Services for more details.			•		
S/MIME v3 0 Secure Multi-Purpose Internet Mail Extensions Version 3	Use MIME when security is not a concern. Use S/MIME encryption when not using the Messaging Transport protocols.				•	
SecureMail	A combination of procedures and standards already listed in the e-GIF required to use the e-government component SEEMail service. See Section 3 E-government Services for more details.		•			

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

2.7   *Best Practice layer*

This section presents international standards and local conventions which 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.

Digital Rights Management (DRM)						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
	Do not enable. See October 2004 paper on Trusted Computing. A Working Group is considering conventions for use across government.		•			

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

Trusted computing						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
	Discussion paper on Trust and Security on the Internet. No convention yet – see EGU Report on Trust & Security. A Working Group is considering conventions for use across government.		•			

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

Process						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
BPEL4WS 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.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

XML data transformation						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
XSLT **eXtensible Stylesheet Language Transformations**	A description vocabulary used by XSL to describe how an XML document is transformed into another XML document.				•	

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

Data modelling						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
UML Unified Modelling Language	Useful for describing objects in a visual format.				•	
XMI XML Metadata Interchange	Enables easy interchange of metadata between odelling tools such as UML and remote metadata repositories.			•		
UBL Universal Business Language	Naming and design rules for schema design.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

Processing structured data						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
SAX Simple API for XML	Parser for large volume repetitious batch transfers. Open standard for navigating and updating XML documents.				•	
DOM Document Object Model	Parser for transactional exchanges. SAX is a Java API for navigating XML documents.			•		

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

Controlled Vocabulary or code Lists (CVLs)						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
CVLs **Controlled Vocabulary or Code Lists)**	Discussion on standardising CVLs. Research underway, led by the ICT Branch of the State Services Commission.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

Health sector						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
HL7 Health Level 7	An international standard adopted by the health sector. Is converging on HL7 Version 2.4 for laboratory results and National Health Index (NHI).		•			

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

Document file format						
Standard	**Comments**	**Status level**				
		F	**U**	**R**	**A**	**D**
ODFOA v1.0, DocBook, WordML Open Document Format for Office Applications Version 1.0, DocBook, Word saved as XML	Several candidates for agencies to save documents in an open, XML format. The Parliamentary Counsel Office's PAL project leads this initiative.	•				

Note: The status level of each protocol is shown as follows: **F** = future consideration; **U** = under development; **R** = re commended; **A** = adopted; **D** = deprecated

3   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 public sector agencies

- compliant with the e-GIF.

The items are:

- **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 websites.

- **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 ICT Branch of the State Services Commission.

- **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

  - The Public Sector Intranet is a pilot provided by the State Services Commission. The Commission is collecting feedback on the pilot and aims to launch it as a full production system in 2006.

- **SEE Mail and SecureMail:** New Zealand Secure Email Requirements; SEEMail and SecureMail

  - Secure email. Two domains are offered:

- SEE Mail is a gateway-gateway crypto layer running over public email, improving confidentiality and authentication. It is intended for use between government bodies (including local government). Note the next version of this service will not accept UUENCODE or TNEF message formats.

- SecureMail is an extension of SEEMail to allow the use of secure email by the New Zealand public.

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

New Zealand E-government

Interoperability Framework

(NZ e-GIF)

Version 3.0

PART 2 – POLICY

March 2006

State Services Commission

About this document

This document outlines the policy behind the e-GIF and its development. The intended audience for this Policy section includes:

- policy analysts

- advisors

- business analysts

- anyone involved with interoperability strategy and projects.

It includes the following sections:

- What is the e-GIF? Short descriptions of e-government, interoperability, and the e-GIF, how the e-GIF will benefit New Zealand, and how the e-GIF is maintained.

- Who must comply and when? Who must comply with the e-GIF, how to transition to e-GIF compliance, exemptions and special provisions.

- Principles: Short descriptions of anticipated outcomes of the e-GIF, requirements for project and operational management, and governance principles.

- Developing the e-GIF: 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.

Table of Contents

1   What is the e-GIF?

The E-government Interoperability Framework (e-GIF) is a set of policies, technical standards, and guidelines. It covers ways to achieve interoperability of public sector data and information resources, information and communications technology (ICT), and electronic business processes. It enables any agency to join its information, ICT or processes with those of any other agency 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 road rules had to be agreed each time one vehicle encountered another.

1.1   What is e-government?

E-government is about government agencies working together to use technology so they can better provide individuals and businesses with government services and information. It is not a massive ICT 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 develop 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.govt.nz/about-egovt/strategy/strategy-june-2003/

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 underscores this 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 takes place.

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

- agencies

- government and people

- government and business.

This does not mean a central agency is simply dictating common systems and processes. Interoperability can be achieved by applying 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 this framework.

1.3   What will the e-GIF accomplish?

Using the e-GIF will:

- help government agencies to work more easily together electronically

- make systems, knowledge and experience reusable from one agency to another

- reduce the effort needed to deal with government online by encouraging consistency of approach

- reduce the reliance on tapes and disks to exchange data, as these carry their own security issues and are not scaleable for the level of interoperability many services will need in future.

1.3.1   Practical example: Consolidating customer resources

Adhering to the e-GIF becomes critical when two or more agencies work together to deliver a service online. Agencies in this situation are encouraged to look at services from a "customer" perspective.

A hypothetical example is opening a café or restaurant. At present, this involves interactions with a number of agencies:

- The Companies Office and Inland Revenue, which provide a shared service for people wanting to start a business. As people incorporate their company, they are able to apply for an IRD tax number. By entering information into the "IRD Details" screen during the online company incorporation process, their application will be sent via an automated link to Inland Revenue. (Until recently new companies had to deal with the Companies Office and Inland Revenue separately).

- Occupational Safety and Health (OSH) for accident forms, hazardous substances 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.

At present, most of this information is available online, but only by visiting each agency's website for its respective services.

Consider this example in an interoperable future: all services for opening a café or restaurant, delivered by multiple agencies, available through a single website: http://www.openingmycaferestaurant.govt.nz . The applicant would enter relevant details, then the agencies would exchange relevant information among 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 achieve such interoperability, the agencies need an enduring, agreed set of standards for exchanging data between all parties. The e-GIF sets out these standards.

(See also Section 3.2, Aims of the e-GIF.)

1.4   Managing the e-GIF

1.4.1   Stewardship

The following people manage the e-GIF:

- The **State Services Commissioner** is the **Steward** of the e-GIF, with accountability and corresponding decision-making authority for its ongoing development and management.

- The **Information and Communication Technologies Branch (ICT Branch)**[1] 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** is made up of public servants from the senior ranks of agencies adopting the e-GIF. The Committee acts for the State Services Commissioner to ensure:

    - the value of the e-GIF as a "collective asset" that supports the future capability and performance of both individual agencies and the public sector as a whole, and one that is maintained and enhanced across time

---

1 The Information and Communication Technologies Branch (ICT Branch) of the State Services Commission, was formed from the E-government unit on 1 July 2005.

- the benefits of the e-GIF (increased agency and public sector capability, performance, efficiency and effectiveness) outweigh its costs (decreased agency-level autonomy, administration costs, etc.).

- **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 take part in its governance and appeal decisions made by the Steward and Management Committee.

1.4.2   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

2.1.1 Mandatory compliance

From 1 July 2002, Cabinet has made using 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.

2.1.2 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 that must or are encouraged to comply with the e-GIF (see Sections 2.1.1 and 2.1.2), 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, and/or

- they are reviewing their overall technology strategy.

See the following sections for details.

2.2.1   Transitions

The adoption of the e-GIF must allow for a sensible transition. Recognising this, Cabinet agreed on 13 June 2002 that current information systems, software applications, or electronic data/information resources did not need to comply immediately with the 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 these, must comply with the e-GIF except 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 an agency has one of these exceptional instances, it needs to consider the customer perspective (see Section 1.3.1). 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 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 most cases, the e-GIF will apply.

2.2.2   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. 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 about the circumstances of the exchange (it may fit with one of the 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 3.3 Governance of shared inputs.

- Part 3, Section 1.10 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

- where sensible, contribute to updating 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.nz/standards/e-gif/faqs.html.

2.3.1 Special provisions

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

3 Principles

3.1 Outcomes for government

The e-government programme seeks the following outcomes, which will be helped by applying 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 adopting the e-GIF and progressively building 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.

3.2 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.

3.2.1 Improving the public face of government

People generally access government services 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 benefit from interoperability. If agency ICT is interoperating effectively, people dealing with public servants face-to-face or on the phone will also receive better service.

3.2.2 Improving agency use of ICT

Adopting common technical standards for ICT means agencies can focus more on the business outcomes the systems are designed to support rather than on technical choices that have little impact on service delivery.

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

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

3.2.3 Operating in a global environment

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

Adopting 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 or global way.

3.3   Governance of shared inputs

Agencies interoperate to:

*   make better use of information and communications technologies (ICT) within government

*   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 ICT Branch of the State Services Commission.

3.3.1   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").

3.3.2   Operational management

There should be some form of agreement for the ongoing operation of any initiative involving more than one agency. The content of the agreement will depend on the nature of the initiative, but the following areas should 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.

3.4   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 take part 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 greater priority.

- Decision-making processes will be transparent.

4 Developing the e-GIF

4.1 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 an agency's specific business needs or for the needs of several agencies in a sector or area of business.

Including these in the framework ensures 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 with the interests of individual agencies and their stakeholders. Where this is not possible, collective interest should be given greater priority.

4.2 Submitting a new standard

The e-GIF is regularly reviewed and updated by issuing a revised version of this document. However, extensions to the e-GIF can be suggested at any time. 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, through 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/standards/e-gif/faqs.html. Note that the agency proposing the standard is expected to take a share in the development and governance of the standard.

4.3 Principles for developing the framework

As well as the principles outlined in this document, a number of guiding principles have been developed for the long-term. For further information email e-gif@ssc.govt.nz.

4.4 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 United Kingdom 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.

4.5 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 (See Part 1, Section 1.1) 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 or for a particular domain, or depend on the use of other standards, or represent high level aggregations of lower level components. One possibility is to include additional descriptions to the standards, 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 Recommended (R) to Emerging (E):** There is some confusion about the word "Recommended" in the current e-GIF compliance status levels (see Part 1, Section 1.3). 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 review cycle information:** Since standards proceed through a cycle of compliant statuses, review cycle information could be included to indicate how long each standard is in force and when it is due for review.

- **Continuous review cycles:** With technology changing constantly, the e-GIF needs to be updated continuously to remain relevant.

- **Using RFC 2119:** This RFC could be used to clarify the interpretation of key words related to the standards. It standardises use of the words "must",

"must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" when specifying requirement level.

New Zealand E-government

Interoperability Framework

(NZ e-GIF)

Version 3.0

PART 3 – RESOURCES

March 2006

State Services Commission

About this document

This document contains resources related to the e-GIF. The intended audience for this Resources section is all readers of the e-GIF.

It includes the following sections:

- History of the e-GIF: Review of stages in the e-GIF's development, including a Change Log.

- References and background information: Descriptions and links to further information related to the e-GIF.

- URLs referred to in the e-GIF: Full URLs for all hyperlinks in the e-GIF.

- Abbreviations: Definitions of abbreviations and acronyms used in the e-GIF.

Table of Contents

1   History of the e-GIF

1.1   The UK e-GIF

The original version of the NZ 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.

1.2   NZ e-GIF v1

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

1.3   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.

1.4   Change Log

1.4.1   Version 3.0 - 3 June 2005

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

- restructured the document, separating Standards, Policy, and Appendixes (Resources)

- added general information about e-government, interoperability, and the e-GIF

- clarified how to comply and included the requirement for data share agreements

- added agency and time limitations to exemption requirements

- revised the layer model to:

    - add Best Practice

    - separate out Web Services

    - change "Architecture" to "Data Integration"

- change "E-government Component Architecture" to "E-government Services" and put it 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 and applying for exemptions, the Roadmap for the e-GIF, and other resources on the Internet

- restructured list of standards and added comments

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

  - Network protocols (TCP/IP), UDP

  - File transfer protocols, WebDAV, SCP

  - Registry services (renamed, was "Registers"), DNS

  - Time, NTP, UTC (MSL)

  - Messaging transport, HTTP 1.1

  - Messaging formats, MIME

  - Primary character set, ASCII

  - Document type definition, DTD

  - Batch/bulk data, CSV

  - File compression, GZIP

  - File archiving, TAR

  - Namespace, URN, OIDS

  - Customer relationship, xCRL

  - E-learning, ADL, SCORM, and IMS

  - Business reporting, xBRL

  - Directory services, DSML

  - Statistical data and metadata, SDMX

  - Geospatial, NZGMS

  - XML 1.1

  - Web services, all components, all standards

  - Instant messaging, XMPP

- Vice Over Internet Protocol, SIP, RTP, H.323, G.711, G.729

- Website presentation, NZ Govt Web Guidelines Version 2.1

- Forms, xForms

- Additional customer information, xCIL, Data formats for identity records standard

- Security (re-sorted components by layer model) - Network, HTTPS, S-HTTP, TLS, IPsec, ESP

- Data integration, XML – Enc

- XML – Dsig or OASIS DSS

- Web services, SAML v2.0, Shared Logon assertion messaging standard

- Shared Workspace

- Government Intranet

- SecureMail

- Best Practice, all components, all standards, added section

- moved the following standards:

  - UDDI, moved to Web Services / Discovery

  - ebXML, moved to Web Services / Messaging

  - Structured data description, RDF, moved to Business services

  - Metadata (Discovery), NZGLS 2.0, NZGLS Thesauri, moved to Business services

  - Unicode, moved; Comment: an extension of ASCII

  - Graphics File, GIF89a, JPG, PNG, SVG, moved to Access and Presentation / Website presentation

  - Mail Attachment, MIME, moved to Network / Messaging formats

  - S/MIME, moved to Security / Business services

  - XSLT, moved to Best Practice / XML data transformation

  - UML, XMI, moved to Best Practice

  - Business services, Metadata (Discovery), RDF, moved from Network / Structured data description

- Business services (continued), Presentation, GIF89a, JPG, PNG, SVG, PDF, moved to Access and Presentation / Website presentation

- Structured data description, RDF, moved to Metadata (Discovery) component

- UML, XMI, moved to Best Practice

- SOAP 1.2, moved to Web Services / Access

- General Text and Graphics, HTML v4.01, GIF89a, JPG, PNG, SVG, PDF, moved to Website presentation (comment)

- UDDI, moved to Web Services / Discovery

- WSDL 1.1, moved to Web Services / Description

- Processing (Structured data), SAX, DOM, renamed, was "Modelling (Structured Data)", moved to Best Practice

- removed the following standard:

  - Autonomy

- revised the following standards:

  - Data integration, renamed, was "Architecture"

  - Structured web document language, HTML v4.01, renamed component, was "Hypertext"

  - Name and address, xNAL v2, specified version

  - Registry services, renamed, was "Registers", ebXML RIM and RS v2.1 and v3.0, specified versions

  - E-government Services, renamed, was "E-government Component Architecture"

  - Content syndication and channel feeds, RSS, renamed component, was "News Syndication"

  - Authentication standards, Evidence of identity, Username / passwords, "Key type 2", Authentication key strengths, Trust levels for online transactions, spelled as out separate standards

  - Business services, S/MIME v3 , specified version.

1.4.2   Version 2.1 - 14 May 2004

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

1.4.3   Version 2.0 - 1 December 2003

This was a substantial rewrite of the e-GIF to clarify its intent and make it more accessible. In particular it:

- introduced a new layer model and removed the old one

- removed the old divisions of Interconnection, Information Sharing and Exchange, Access, and Service Delivery and reclassified standards into Network, Architecture, Business Services, and Access and Presentation

- added a list of e-Government components

- replaced the terms Standards and Guidelines with Mandatory and Recommended to clarify intent

- reclassified all standards in the move to version 2; in addition, the status of the following standards was changed:

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

  - corrected XSL to XSLT under data transformation services.

  - added version number on ZIP compression standard – now ZIP 2.3.

  - added xNAL as Mandatory standard for Name and Address data transfers.

  - made SAX a Mandatory standard (was a guideline, now called Recommended) for modelling structured data.

  - added New Zealand Government RSS as a future standard for news syndication.

  - added a placeholder for authentication standards with a note to seek EGU advice.

  - updated reference to New Zealand Government Web Guidelines to current version (v2.1).

  - added note about SecureMail as potential future government-to-citizen hardened email standard.

  - added lists of EGU components – available and under development.

1.4.4   Version 1.1 - 3 July 2003

Added ESA as a Recommended standard.

1.4.5   Version 1.0 - 13 June 2002

Initial release of e-GIF.

2   References and background information

2.1   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.govt.nz/about-egovt/strategy

2.2   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.

2.3   Privacy Act 1993

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

2.4   Security in the Government Sector

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

2.5   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.govt.nz/standards/e-gif/data-management-policies

http://www.e.govt.nz/standards/e-gif/data-management-standards

http://www.e.govt.nz/standards/e-gif/is-policies-standards

URLs referred to in the e-GIF

This document refers to a range of resources on the Internet, including:

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

These links are listed in full in the following sections.

2.6   Standards

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.govt.nz/services/authentication

BPEL4WS
http://www128.ibm.com/developerworks/library/specification/ws-bpel/

CSV
http://www.answers.com/main/ntquery?method=4&dsid=1512&dekey=com
ma+delimited&gwp=8&curtab=1512_1

CVLs
http://www128.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.oasisopen.org/committees/tc_home.php?wg_abbrev=docbook

DOM
http://www.w3.org/DOM/

DRM
http://www.e.govt.nz/policy/trust-security/trusted.html (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.oasisopen.org/committees/tc_home.php?wg_abbrev=ebxml-msg

ebXML RIM and RS V2.1 & v3.0
http://www.oasisopen.org/committees/tc_home.php?wg_abbrev=regrep

ESA
http://www.linz.govt.nz/rcs/linz/pub/web/root/core/Topography/ProjectsAnd
Programmes/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)

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)

G.711
http://en.wikipedia.org/wiki/G.711

G.729
http://en.wikipedia.org/wiki/G729

GCSB NZSITs
http://www.gcsb.govt.nz/publications/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.323 v2
http://en.wikipedia.org/wiki/H323
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

IPsec
http://www.ietf.org/rfc/rfc2402.txt
http://www.ietf.org/rfc/rfc2404.txt (IP Security Authentication Header)

IP v4
http://www.ietf.org/rfc/rfc0791.txt

IP v6
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.govt.nz/standards/nzgls/management/

MIME
http://www.ietf.org/rfc/rfc2049.txt

NTP 4.0
http://www.ntp.org/

NZGLS 2.0
http://www.e.govt.nz/standards/nzgls/standard

NZGLS Thesauri
http://www.e.govt.nz/standards/nzgls/thesauri

NZGMS
http://www.e.govt.nz/standards/e-gif/nzgms

NZ Govt Web Guidelines 2.1
http://www.e.govt.nz/standards/web-guidelines

OASIS DSS
http://www.oasisopen.org/committees/tc_home.php?wg_abbrev=dss

ODFOA 1.0
http://www.oasisopen.org/committees/tc_home.php?wg_abbrev=office

OIDS
http://en.wikipedia.org/wiki/Object_identifier

OpenSAML
http://www.opensaml.org/

PAL project
http://www.pco.parliament.govt.nz/pal/

PDF
http://www.adobe.com/products/acrobat/adobepdf.html

PNG
http://www.libpng.org/pub/png/

Portal News Feed
http://www.e.govt.nz/standards/e-gif/rss

RDF
http://www.w3.org/RDF/

RSS
http://web.resource.org/rss/1.0/

RTP
http://www.ietf.org/rfc/rfc3550.txt

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/services/securemail
SEEMail
http://www.e.govt.nz/services/see

SEE PKI
http://www.e.govt.nz/services/see (SEE)

Shared Workspace
http://www.e.govt.nz/services/workspace

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/rfc/rfc3261.txt
http://computing-dictionary.thefreedictionary.com/codec (Codec)

S/MIME v3.0
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 1.1
http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

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/policy/trust-security/trust-security-2004/index.html
(Discussion   paper   on   Trust   and   Security   on   the   Internet),
http://www.e.govt.nz/policy/trust-security (SSC Report on Trust & Security)

UBL
http://www.oasisopen.org/committees/sc_home.php?wg_abbrev=ubl-ndrsc

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
589232_1.DOC - Namespace
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 Format)

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.oasisopen.org/committees/tc_home.php?wg_abbrev=wss

WSDL 1.1
http://www.w3.org/TR/2001/NOTE-wsdl-20010315

WSE2
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/

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/standards/e-gif/xnal

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/

2.7 e-GIF documents

December 2001 New Zealand E-government Strategy
http://www.e.govt.nz/about-egovt/programme/e-gov-strategy-dec-01/

June 2003 E-government Strategy Update
http://www.e.govt.nz/about-egovt/strategy/strategy-june-2003/

Current version of the e-GIF
http://www.e-gif.govt.nz

Roadmap for the e-GIF
http://www.e.govt.nz/standards/e-gif/e-gif-roadmap

Frequently Asked Questions and Answers about the e-GIF
http://www.e.govt.nz/standards/e-gif/faqs.html

2.8 Other New Zealand Government documents

New Zealand Government Data Management Standards
http://www.e.govt.nz/standards/e-gif/data-management-standards

New Zealand Government Data Management Policies
http://www.e.govt.nz/standards/e-gif/data-management-policies

New Zealand Government Information Systems Policies and Standards
http://www.e.govt.nz/standards/e-gif/is-policies-standards

NZ Govt Web Guidelines 2.1
http://www.e.govt.nz/standards/web-guidelines/web-guidelines-v-2-1

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/policy/trust-security/trusted.html

SSC Report on Trust and Security
http://www.e.govt.nz/policy/trust-security/trust-security-2004

2.9   Other resources

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/

Wikipedia (Definitions for protocols)
http://en.wikipedia.org/wiki/Protocol_%28computing%29
http://en.wikipedia.org/wiki/Communications_protocol

RFC 2119 (Key words for use in RFCs to indicate requirement levels)
http://www.faqs.org/rfcs/rfc2119.html

3   Abbreviations

The following abbreviations and acronyms are used in the e-GIF v3.0.

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

ESA Emergency Services in Government Administration

ESP IP Encapsulation Security Protocol

FTP File Transfer Protocol

GCSB Government Communications 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

ICT Branch Information and Communication Technologies Branch of the State Services Commission

IMS Instructional Management System

IPsec IP Security Authentication Header

ITU-T International Telecommunication Union – Telecommunication Standardization Sector

LDAP Lightweight Directory Access Protocol

MIME Multi-purpose Internet Mail Extensions

NAT Network Address Translation

NTP Network Time Protocol

NZGLS New Zealand Government Locator Service

NZGMS 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 (Open Document)

OIDS Schema Object Identifiers

PKI Public Key Infrastructure

PNG Portable Network Graphic

RDF Resource Description Framework

RSS Rich Site Summary

RTP Real-time Transport Protocol

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

S/MIME Secure Multi-purpose Internet Mail Extensions

SMTP Simple Mail Transfer Protocol

SOAP Simple Object Access Protocol

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 Uniform Resource Name

UTC (MSL) Universal Time Clock (Measurement Standards Laboratory)

UTF Unicode Transformation Format

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